HORIZON-HLTH-2022-IND-13-01

NEMECYS [101094323]: New Medical Cybersecurity assessment and design solutions

D5.1 Dissemination & Communication Plan

Project Reference No	NEMECYS – 101094323
Deliverable	D5.1 Dissemination & Communication Plan
Work package	WP5: Dissemination, Exploitation and Outreach
Type	R - Document, report
Dissemination Level	PU - Public (fully open)
Date	28/04/2023
Status	Final v1.0
Editor(s)	George Zissis (ATC)
Contributor(s)	Karin Bernsmed (SINTEF)
Reviewer(s)	Mariet Nourijanian (OSR), Alice Leporini (OSR), Colin Upstill (ICE), Martin Gilje Jaatun (SINTEF)
Document description	The Dissemination and Communication Plan is a living document/ manual for the NEMECYS project partners' dissemination and communication activities.

Disclaimer

The NEMECYS project is co-funded by the European Union under grant agreement ID 101094323. The information and views set out in this publication are those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Document Revision History

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
V0.1	10/03/2023	TOC	George Zissis (ATC)
V0.2	17/03/2023	Draft content	Karin Bernsmed (SINTEF)
V0.3	03/04/2023	1st complete draft	George Zissis (ATC)
V0.4	19/04/2023	Updated draft	Mariet Nourijanian (OSR), Alice Leporini (OSR), George Zissis (ATC)
V0.5	20/04/2023	Review of the draft	Collin Upstill (ICE), Karin Bernsmed (SINTEF), Martin Gilje Jaatun (SINTEF)
V1.0	28/04/2023	Final version	George Zissis (ATC)

Executive Summary

This document sets out the dissemination and communication plan to raise awareness, share knowledge, and attract potential stakeholders in the context of the NEMECYS project. This shall be achieved through various means, including the NEMECYS website, the use of social media, the distribution of communication material, publications in journals, participation in conferences and other relevant events, and organization of stakeholder events. The report provides a comprehensive framework for actions that will support outreach efforts necessary to disseminate and sustain the achievements and benefits of the NEMECYS project. It provides a focused dissemination and communication approach towards the key target audiences and the best approaches to engage and inform stakeholders to maximize knowledge of NEMECYS activities.

Table of Contents

List of Figures

List of Tables

List of Terms and Abbreviations

Abbreviation	Definition
CMD	Connected Medical Device
EU	European Union
HADEA	European Health and Digital Executive Agency
MDCG	Medical Device Coordination Group
R&D	Research and Development

1 Introduction

This dissemination and communication plan provides a comprehensive framework for actions that will support outreach efforts necessary to disseminate and sustain the achievements and benefits of the NEMECYS project. It provides a focused dissemination and communication approach towards the key target audiences and the best approaches to engage and inform stakeholders to maximize knowledge of NEMECYS activities. The current document enables the reader to have a clear understanding of both the difference and the overlap between communication and dissemination audiences and tools when we combine the two concepts into one overall strategy as presented in the next chapters of the deliverable.

1.1 Purpose and Scope

The NEMECYS project addresses the interests of a wide range of stakeholders in the lifecycle of connected medical devices. These stakeholders can be reached through the organizations and groupings in which they meet and gather. These "communities" are the groups that NEMECYS will target for dissemination and communication. The purpose of this document is to outline the plan that will be implemented during and after the project lifetime to engage with these communities.

1.2 Methodology and Structure of the Deliverable

This document will be a living document, which will be used to coordinate and align all communication and dissemination in the project. There is only one official deliverable of this document: D5.1 Dissemination and Communication Plan (due at M4: April 30th, 2023), but the document will be updated on a regular basis and utilized during the whole lifetime of the project.

The document is outlined as follows:

- Section 2 outlines the NEMECYS dissemination and communication strategy.
- Section 3 presents the NEMECYS brand identity.
- Section 4 describes the target audience and the NEMECYS-specific stakeholder groups.
- Section 5 explains our dissemination and communication tactics.
- Section 6 contains a time-plan for the different periods of the NEMECYS communication and dissemination actions.
- Section 7 provides the means and indicators for the dissemination and communication monitoring.
- Section 8 outlines the EU rules to be followed by the project partners related to the co-funding acknowledgement.
- Section 9 presents the roles and responsibilities of the NEMECYS partners related to the project's dissemination and communication tasks.
- Section 10 provides the conclusions of the current document.
- The final section of this report contains four annexes with the list of stakeholders, relevant journals, applicable events, and sibling projects.

2 NEMECYS Dissemination and Communication Strategy

2.1 Objectives

NEMECYS aims at the development of new cybersecurity assessment techniques and tools for security-by-design for connected medical devices (CMDs). NEMECYS will benefit practitioners such as cybersecurity communities, CMD manufacturers, CMD scenario system integrators and CMD scenario operators (e.g., health care providers), with downstream benefits to patients and the wider public, through more cost-effective and efficient care enabled via effective and streamlined cybersecurity. Toward this end, NEMECYS's central dissemination objectives are to:

- Engage potential stakeholders, particularly cybersecurity experts, CMD manufacturers, integrators, operators such as hospitals and health care providers, researchers, and developers.
- Bring together and reinforce links between the CMD industry, the cybersecurity community, health care providers, policymakers, regulators and researchers.
- Present the project progress and results outside the scope of the NEMECYS consortium, ensuring awareness amongst a broad range of stakeholders.
- Establish the basis for long-lasting interest and commitment to privacy and security in the CMD industry and health care sector.
- Establish liaisons/synergies with other R&D projects and thematic networks at national and EU levels.

2.2 Strategy

The dissemination and communication strategy of the NEMECYS project will consist out of three consecutive periods. The three different periods require different methods and activities to be undertaken in order to achieve their goals:

1. The awareness-oriented period aims at creating stakeholders' awareness and to raise public interest. During this period, a dissemination and communication plan will be developed, a public website will be created, project information material (such as a poster and leaflet) designed and introductory presentation and workshops to raise the awareness of the stakeholders. This period will coincide with the first year of the project; most activities will start immediately.
2. The result-oriented period will promote the results of the project to (potentially) interested parties (including the scientific audience). During this period, public deliverables and news will be displayed on the project website for viewing and downloading in order to show the progress of the project and to keep the stakeholders updated. In addition, high quality papers will be submitted to scientific journals and presentations given at conferences and workshops. After completing important milestones, the consortium will publish press releases and social media posts.
3. The sustainability & wider dissemination period will deploy specific activities in order to ensure the sustainability of the project outcomes. To this end, a sustainability plan will be elaborated in order to ensure the continuation of the NEMECYS project outcomes. During this period, NEMECYS partners and involved stakeholders e.g. the NEMECYS community, will define pathways for the continuation of the communication and future evolution of the project' results.

In order to accommodate the internal variations in interest between audience groups, the project has devised a two-tiered strategy to reach its target audience and achieve communication and dissemination objectives:

1. Large scale mass communication and awareness-raising,
2. Targeted in-depth and long-term dissemination.

Toward this end, NEMECYS approaches dissemination from two orthogonal dimensions:

- Horizontal (large scale) communication to raise awareness and reach out to the wider stakeholder groups interested in cybersecurity in the health care sector and particularly for connected medical devices;
- Vertical (targeted) dissemination to consolidate the community and the knowledge base between stakeholders.

As detailed in Table 1 and the following sections, NEMECYS uses a blend of online and offline tactics to deploy an integrated dissemination approach according to which the project systematically maps and reaches stakeholders and audiences via online communities (such as LinkedIn) as well as offline channels (such as conferences and workshops):

Table 1: Online and offline tactics

	NEMECYS	Other
Online	NEMECYS website, social media (Twitter, LinkedIn, Mastodon)	Existing online communities' social media related to NEMECYS project objectives.
Offline	NEMECYS thematic and stakeholder events, dissemination conference, marketing material	Participation in existing events and conferences

3 NEMECYS Brand identity

The brand is the perceived image of the project, and it is conceived to tell the audiences about NEMECYS' story, its growth, innovative elements and aims. The identity of a project is vehiculated by visual tools used to represent the brand with consistency and coherence. All the digital and printed elements regarding Brand Identity, such as the logo, the website, templates, presentations and posters of the project, must have a coordinated image. In the following, the guidelines chosen for NEMECYS and their rationale are described.

3.1 Project Logo

Branding is essential to enhance visibility and awareness of a project and business in general. The logo is one of the main graphic identity elements of the NEMECYS project and a key to build a successful dissemination campaign. The logo is included in all graphic material and documents related to the project. Therefore, the design of the NEMECYS logo has been carried out in a way that it can be representative of the project objectives and results. Table 2 presents the main characteristics of the project logo, which is seen in Figure 1.

Table 2: Main characteristics of the project logo

Objective	A visual representation of the reference to cyber security and CMDs.
Key message	Provide awareness and visibility of the NEMECYS project.
Target stakeholder(s) / audience	All target stakeholders and all audiences
Content provider	The project logo has been selected from different logos suggested by OSR and ATC.
Frequency of content update	The project logo is designed once to maximize visibility.
Feedback and follow-up activity	The project logo is mainly used to engage stakeholders and promote project objectives and activities.

Figure 1: The NEMECYS project logo

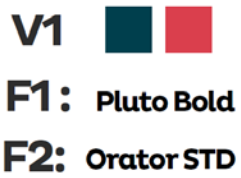

Figure 2: NEMECYS Chromatic Palette and Font

3.1.1 The sign

The sign is the intuitive part of the logo, and the one of highest visual impact. It is made of two contrasting parts. In the foreground we have a red cross to represent the healthcare sector of the project. By contrast, a geometrical figure lies in the background: the shield, a complex image that convey the idea of security, rigor and complexity.

3.1.2 The colour palette

We chose two colours which, as the elements mentioned above, are in opposition to each other: *(i)* a tone of blue (Iris Blue), the typical colour used in healthcare for its ability, attested by colour psychology, to normalize the heartbeat frequency and blood pressure, and to remove the sense of anxiety; *(ii)* and a tone of yellow (Ronchi), symbol of sunlight but also of knowledge and energy (see Figure 2). Again, combining two contrasting colours amounts to imposing a visual energy force on the composition.

3.2 Visual Identity Kit

To ensure a consistent appearance, a visual identity kit for the project has been developed. The visual identity kit consists of templates and the NEMECYS Brand Manual to be used by the partners when generating the material for the dissemination and communication activities in the project.

3.3 Project PowerPoint Presentation

The project has created an introductory PowerPoint presentation, which will be used to introduce the objectives and expected results from the project to external parties in, for example, networking activities, workshops, and events. The presentation can be used by any of the project partners, both in their internal communication activities as well as when communicating with external stakeholders and audiences. The presentation will be updated during the course of the project when new results etc. become available. Table 3 presents the main characteristics of the PowerPoint presentation and the title slide of the presentation of is seen in Figure 3.

Table 3: Main characteristics of the introductory PowerPoint presentation

Objective	To provide a light-weight introduction to the project.
Key message	Provide awareness and visibility of the NEMECYS project objectives and expected results.
Target stakeholder(s) / audience	Stakeholders and audiences participating in networking activities, workshops, and events.
Content provider	All partners can propose updates, but SINTEF will maintain it.
Frequency of content update	At regular time intervals, when new results become available.
Feedback and follow-up activity	The project partners in the WP5 team will ensure timely updates of the presentation content.

Figure 3: The title slide of the introductory presentation of the NEMECYS project

3.4 Project Brochure

Table 4: Main characteristics of the project brochure

Objective	To outline the project key objectives and expected outcomes. The brochure should be distributed at all dissemination events, conferences, workshops.
Content and messages	Project's background; invitation for the stakeholders to visit the website and join NEMECYS on social media.
Target audience	All Stakeholders
Information required	The master document will be drafted in English
Information provider	The master document will be made by ATC based on partners' contribution
Communication methods	Written communication, face to face distribution, internet
Activities	Writing content, designing, editing and printing the document
Schedule	Revision throughout the project duration if necessary
Monitoring	ATC in collaboration with the other partners will monitor the production and dissemination of the brochure.
Responsible partner	ATC is responsible for the master version

3.5 Project Poster

Table 5: Main characteristics of the project poster

Objective	The main purpose of the poster is to explain the project and its objectives in a simple and accessible way. To reach this objective an eye-catching poster will be designed. The poster will be used in all dissemination events, conferences and project workshops.
Content and messages	Project background; invitation for the stakeholders to visit the website and join NEMECYS on social media.
Target audience	All Stakeholders
Information required	The master document will be drafted in English
Information provider	The master document will be made by ATC
Communication methods	Internet, face to face for presentations, events
Activities	Writing content, designing, editing and printing the poster
Schedule	Revision throughout the project duration if necessary
Monitoring	ATC in collaboration with the partners will monitor the production and dissemination of the poster.
Responsible partner	ATC is responsible for the master version

3.6 Project Banner

Table 6: Main characteristics of the Project Banner

Objective	The main purpose of the banner is to catch the audience attention. To reach this objective an eye-catching banner will be designed. The banner will be used in all dissemination events, conferences, project workshops.
Content and messages	Project background; invitation for the stakeholders to visit the website and join NEMECYS on social media
Target audience	All stakeholders
Information required	The master document will be drafted in English
Information provider	The master document will be made by ATC
Communication methods	Internet, face to face for presentations, events
Activities	Writing content, designing, editing and printing the poster
Schedule	Revision throughout the project duration if necessary
Monitoring	ATC in collaboration with the partners will monitor the production and dissemination of the banner.
Responsible partner	ATC is responsible for the master version

4 Target Stakeholder Groups and Audience

4.1 Defining the Target Stakeholders and Audiences of NEMECYS

Stakeholders are any single person or group that can relate to the project and its results. Stakeholders are therefore the individuals, groups of individuals and the organizations that affect, or could be affected, by the NEMECYS project and its results.

4.2 Target Stakeholders and Audiences in NEMECYS

The target groups of stakeholders in the results of the project are first and foremost in the healthcare industry, in particular CMD manufacturers, suppliers and integrators, and health care providers and operators. Other targeted groups are advisory bodies (notably the MDCG), notified bodies, and regulators. An important additional target group is cybersecurity experts from various domains and also professionals from other sectors and applications where IoT devices share confidential or sensitive data. Finally, the project results are also relevant for a wider audience, including patients, the general public and the society as a whole.

Table 7 provides a structured breakdown of the broad stakeholder groups relevant for the NEMECYS project, the specific stakeholders identified within these groups, and our goals for dissemination and

communication towards them. As seen in the table, the identified stakeholders are a mix of different communities, organizations, industry bodies, regulatory bodies and advisory groups.

A detailed list of these target stakeholders and audiences, including their full name and URLs, who in the NEMECYS consortium is in contact with them, and what type of relationship they have, is provided in Annex 11.1.

Table 7: Main characteristics of the NEMECYS stakeholder groups

Stakeholder groups	Identified stakeholders	Desired outcome of the D&C activities
CMD manufacturers	AdvaMed, Aleap, EIT Health, MDIC, MTE	Awareness of the need for cyber security, potential vulnerabilities of their devices and how to address them
CMD suppliers	AdvaMed, Aleap, EITh Health, MDIC, MTE	Awareness of the need for cyber security, potential vulnerabilities of their devices and how to address them
System integrators	AdvaMed, Aleap, EIt Health, MDIC, MTE, NSSC	Awareness of the need for cyber security, potential vulnerabilities of their devices and how to address them
Healthcare providers and operators	Avisados, Gruppo San Donato, HIMSS, Health-ISAC, HSCC, Norway Health Tech, MTE, NOMA, NSSC	Awareness of research results related to cyber security and CMDs.
Advisory bodies	Access Partnership, Norwegian Ethics Committee	Feedback on our suggested improvements to the MDCG guidelines. Feedback on our tool kits.
Notified bodies	DNV (Norway)	Feedback on our suggested improvements to the MDCG guidelines. Feedback on our tool kits.
Regulators	IMDRF	Feedback on our suggested improvements to the MDCG guidelines. Feedback on our tool kits.
Cyber security experts	AISP, CCAPAC, DSAC, ECSO, ENISA, NESSI, InfraGard, NCSC	Awareness of research results related to cyber security challenges and solutions in the medical domain.
IoT and big data communities	AIOTI, BDVA	Awareness of research results related to the use of IoT devices and big data in the medical domain.
The wider audience	Avisados, Norway Health Tech	Awareness of project results on a more general level

5 Dissemination and Communication Tactics

To ensure the effectiveness of dissemination and communication activities, the NEMECYS project has identified multiple channels and means for promoting the project and spreading the project achievements and results to the identified target stakeholder groups and the project's audience. These comprise both online and offline activities.
The main dissemination activities include:

- Scientific publications
- Conferences and events
- Workshops
- Final conference
- Connecting with existing EU initiatives

The main communication activities include:

- Project website
- Social media

5.1 Dissemination Activities

5.1.1 Scientific Publications

As part of the scientific dissemination, the NEMECYS project partners will publish relevant findings in scientific conferences and workshops, where we will present and demonstrate research results from the project. Appendix 11.2 presents a list of an indicative list of relevant events, which the project participants target to attend during the project.

Furthermore, NEMECYS partners will aim to publish the results of the conducted research will also to refereed journals to maximize the impact of the scientific work to the target research communities. Annex 11.3 provides a list of targeted refereed journals in the respective fields.

5.1.2 Conferences and Events

Table 8: Main characteristics of the conferences and events

Objective	To increase the project's visibility by participating in relevant conferences and events, to inform stakeholders about NEMECYS.
Content and messages	NEMECYS challenges, vision, results and outcomes
Target audience	Cybersecurity experts, MD manufacturers, CMD system integrators, health care operators such as hospitals or care providers, policy-makers/regulators, researchers and academics.
Information required	Function of the specific event
Information provider	Partner(s) attending the event
Communication methods	Speech presentation, distribution of dissemination material
Activities	Preparation of the dissemination material according to the specific event
Schedule	This is an ongoing process starting from month 1 till the end of the project.
Monitoring	All Partners organizing/attending the conferences/events will report to ATC the main results of the related activities.
Responsible partner	All partners

5.1.3 Workshops

Table 9: Main characteristics of the NEMECYS thematic workshops

Objective	Organisation of thematic workshops for CMD manufacturers, CMD system integrators, health care operators and the NEMECYS partners focusing on the specific needs for cybersecurity for connected medical devices.
Content and Messages	Project updates, challenges and developments in cybersecurity for connected medical devices.
Target Audience	CMD industry, integrators, health care operators, regulators, cybersecurity experts and researchers.
Information Required	Main project documentation and material; medium to high level detail
Information Provider	ATC, SINTEF and all partners
Communication Methods	Social media, e-mail
Activities	Organising logistics, inviting speakers and participants, managing the workshops (content, presentations timing, moderation etc.)
Schedule	At least 3 thematic workshops are envisioned during the lifetime of the project
Monitoring	SINTEF, ATC and WP5 partners
Responsible Partner	All partners involved in this task will collaborate by facilitating contact, interactions and supporting the organizations of the meetings.

5.1.4 Final Conference

Table 10: Main characteristics of the NEMECYS Final Conference

Objective	NEMECYS envisions to organise one international conference to disseminate project final results
Content and Messages	Project final results, challenges and developments in cybersecurity for connected medical devices
Target Audience	EU and National Regulatory bodies and Authorities; Researchers, Academics and cybersecurity experts, CMD Manufactures and Integrators, Health Care Providers.
Information Required	Main project documentation and material; medium to high level detail
Information Provider	SINTEF, ATC and NEMECYS partners
Communication Methods	Social media, e-mail
Activities	Organising logistics, inviting speakers and participants, managing the conference
Schedule	TBD
Monitoring	SINTEF, ATC and WP5 partners
Responsible Partner	All partners

5.1.5 Connecting with Existing EU Initiatives

All projects funded under the HORIZON-HLTH-2022-IND-13-01 topic have been strongly encouraged to participate in networking and joint activities, as appropriate. The purpose is to exchange information and ideas with each other and explore potential synergies in the area of the topic. In total five project were funded under this topic and our four "sibling" projects are:

- SEPTON, coordinated by SPACE HELLAS SA (EL).
- CYCLOMED, coordinated by CHARITE (DE).
- MEDSECURANCE, coordinated by UNPARALLEL INNOVATION LDA (PT).
- ENTRUST, coordinated by UNISYSTEMS LUXEMBOURG SARL (LU).

The collaboration with these four projects has already begun and will continue throughout the project lifetime.

In addition, there are many other existing EU initiatives, which will also be highly relevant for the NEMECYS project. Annex 11.4 provides a list of the ones that have been identified so far. These may be brought into the list of targeted stakeholders at a later stage, if appropriate.

5.2 Communication Activities

5.2.1 Project Website

A strong online presence will ensure the visibility of the project and knowledge accessible to multiple audiences. The NEMECYS website will be a stable access point for multiple audiences with sections targeted to the general public as well as specialized sections addressing the scientific community and other stakeholders. It will be supported by a set of tailor-made infographics suitable for science-to-public communication. The website will be officially released during the spring of 2023[1] under the https://nemecys.eu/ domain.

The main characteristics of the NEMECYS website are presented in Table 11 below.

Table 11: Main characteristics of the project website

Objective	Act as the main dissemination and communication channel for the project
Key message	An online meeting point for cybersecurity of connected medical devices
Target stakeholder(s) / audience	All target stakeholders and all audiences
Content provider	All partners
Activity required for production and delivery	Gathering content from all partners and outside sources.
Frequency of content update	Following a review process for content publication.
Feedback and follow-up activity	Gather comments/content from NEMECYS consortium. Partner ATC (WP5 leader) uploads/updates the content and performs regular maintenance of the site, as needed.

5.2.2 Social Media

Social media is nowadays one of the primary means for communicating the objectives, activities and results for any EU project. At the time of writing, we have established a Twitter account, a LinkedIn page, and a Mastodon account. Here, periodic updates on events, milestones, and achievement, ranging from short announcements to longer podcasts, will be published to increase the impact of NEMECYS. Short news, updates or complementary links associated to the project will also be published, using a list of relevant hashtags.

5.2.2.1 LinkedIn Page

A LinkedIn page dedicated to the NEMECYS project has been created. The page targets all the professionals in the LinkedIn world who belong to the stakeholder groups as presented in Table 7, and are interested in relevant issues, to share news, discussion and related content. We will encourage project

[1] The official due date of the deliverable "D5.6 Project public website" is at M6: June 30th, 2023.

members to actively use their own LinkedIn profiles to build the NEMECYS community on LinkedIn. This will be our primary social media channel.
The website will include a link to the project's LinkedIn page on the home page.
The main characteristics of the LinkedIn group are presented in Table 12.

Table 12: Main characteristics of the project LinkedIn page

Objective	Informative communication channel complementary to the NEMECYS website.
Key message	Open forum for exchange and discussions related to cybersecurity issues in CMDs among relevant stakeholders.
Target stakeholder(s) / audience	Relevant stakeholders and audiences using LinkedIn.
Content provider	All partners.
Activity required for production and delivery	• Provide highlights of the project. • Inform on any relevant news. • Publish content for stakeholder engagement.
Frequency of content update	On-going
Feedback and follow-up activity	Check comments from the group members

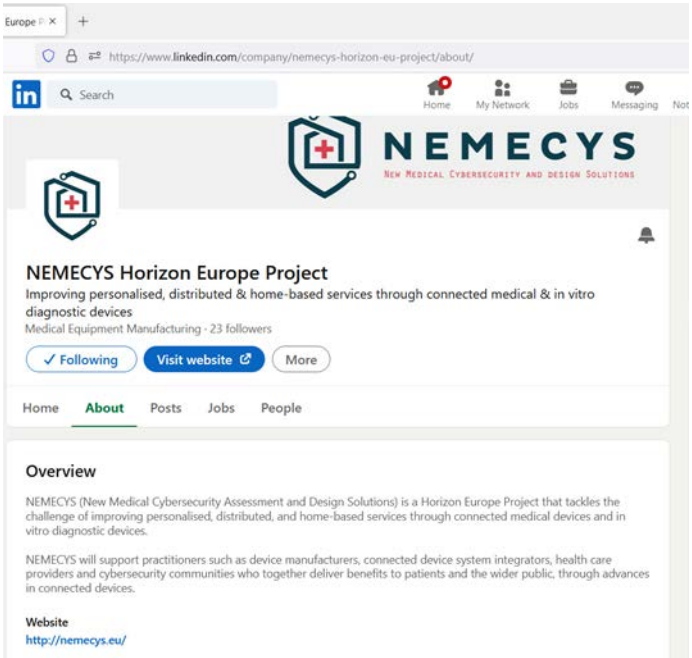

Figure 4: NEMECYS LinkedIn Page

5.2.2.2 Twitter Feed

The Twitter account " NEMECYS_EU" has been created and it will be used to provide short news updates and other tweets about the project. The project Twitter feed will be secondary channel in support of the website and LinkedIn presence, which will be exploited by all partners. The website will maintain a Twitter widget on the home page.

The main characteristics of the Twitter feed are presented in Table 13.

Table 13: Main characteristics of the project Twitter feed

Objective	Show active presence in one of the most popular social media networks.
Key message	There is always something happening in the context of the NEMECYS project. It's worth following the project and its results.
Target stakeholder(s) / audience	Relevant stakeholders and audiences present on Twitter.
Content provider	All partners.
Activity required for production and delivery	Project partners need to summarize relevant content in short text
Frequency of content update	On-going.
Feedback and follow-up activity	Communication with followers.

Figure 5: NEMECYS Twitter account

5.2.2.3 Mastodon Account

In addition to the Twitter account a Mastodon Account has been created and similarly will be used to provide news and updates about the NEMECYS project. Mastodon is an open-source decentralized social media platform and will allow increased visibility of the NEMECYS project and its outcomes.

Table 14: Main characteristics of the NEMECYS Mastodon account

Objective	Show active presence in an open-source decentralized social media platform (Mastodon).
Key message	There is always something happening in the context of the NEMECYS project. It's worth following the project and its results.
Target stakeholder(s) / audience	Relevant stakeholders and audiences present on Mastodon.
Content provider	All partners.
Activity required for production and delivery	Project partners need to summarize relevant content in short text
Frequency of content update	On-going.
Feedback and follow-up activity	Communication with followers.

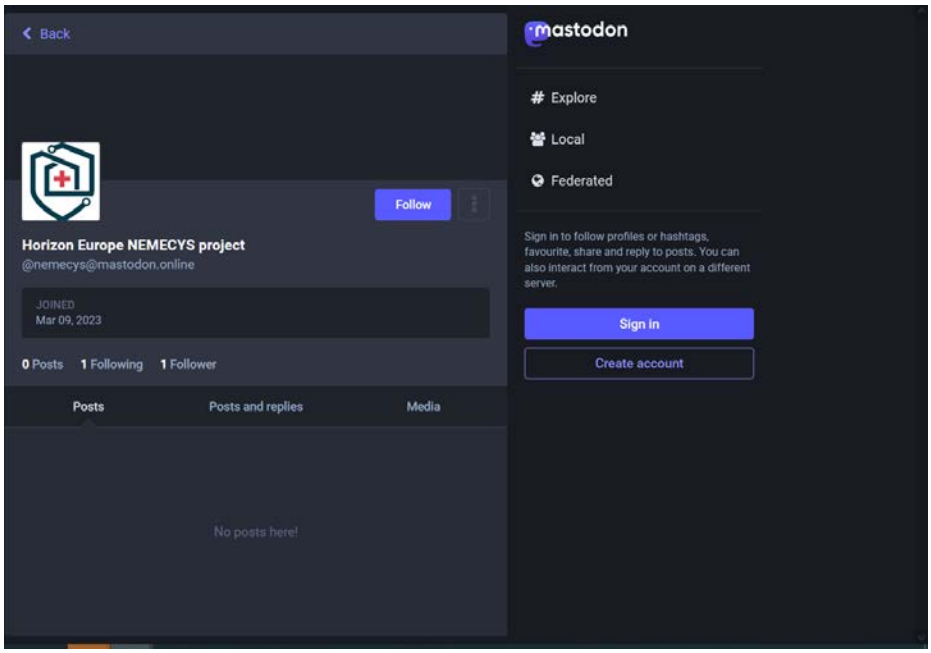

Figure 6: NEMECYS Mastodon account

6 Dissemination and Communication Time-Plan

The planning for the communication and dissemination of the project has started off at a fairly high level and will be continuously refined and updated during the project lifecycle as new opportunities for

communication and dissemination arise. For ease of delivery, the activities have been broken down into three periods:

1. Awareness-oriented period
2. Result-oriented period
3. Sustainability & wider dissemination period

The rest of this section outlines the plans for key activities foreseen for the three aforementioned periods. The plan will be regularly updated throughout the project.

Table 15: Plan for key activities

Period	Goals	Planned Activities	Expected Results & Outputs	Dates
Period 1: Awareness-oriented period	• Build the NEMECYS brand name • Produce key dissemination material • Create awareness about the project's vision and objectives • Start engaging stakeholders	• Produce strategic communication messages • Produce key dissemination material • Build the NEMECYS website, LinkedIn and Twitter • Start Engaging stakeholders • Preparation of publications for international conferences, journals, and specialized magazines • Project Presentations at international conferences • Liaison with sibling projects	• Logo production • Creation of the website • Establishment of social network presence • Creation of key dissemination material (brochure, poster, banner) • Project presentations and publications • Stakeholder map and Communication & Dissemination Plan • Projects liaisons • Collaboration with related communities focused on cybersecurity for CMD	M1-M12

Period	Goals	Planned Activities	Expected Results & Outputs	Dates
Period 2: Result-oriented period	• Leverage the participation of different stakeholders; • Reaching out to the wider community of non-experts	• Engage stakeholders to assist with the dissemination of the project results • Set-up of the NEMECYS Social Media communities • Ensure active stakeholder feedback • Support liaison activities with other cybersecurity for CMD projects • Organize project's thematic events. • Preparation of publications for international conferences, journals	• Social Media posts regularly published • Production of press releases at national and EU level • NEMECYS thematic workshops and events • Project presentations and publications	M12- M24

Period	Goals	Planned Activities	Expected Results & Outputs	Dates
Period 3: Sustainability & wider dissemination	• Disseminate final NEMECYS activities and outcomes	• Website updated • Production of several press releases • Production of related articles and presentations • Preparation of publications for international conferences and journals. • Organize project's thematic events • Establish contact with CMD manufacturers, integrators and operators. • Presentations to CMD industry, related associations and regulatory authorities.	• Social Media posts regularly published • Production of press releases at national and EU level • NEMECYS thematic workshops and events • Project presentations and publications • Elaboration of a plan for continuation of the NEMECYS cybersecurity community communication.	M24-M36

7 Dissemination & Communication Activities Monitoring

7.1 Quantitative & Qualitative Evaluation of NEMECYS Dissemination and Communication

In accordance with the evaluation indicators for measurement of the level of success of communication and dissemination activities, the qualitative and quantitative aspects of evaluation will be examined in detail in the following paragraphs.

In order to capture the effectiveness of communication, a combination of indicators and feedback mechanisms will be used to measure the effectiveness of each communication and dissemination activity, so that an aggregating record is kept and described in the relevant deliverables (D5.3 and D5.4 Report on Dissemination and Communication Activities, first and final). Information to be contained in these reports (D5.3 and D5.4) is as following:

Table 16: Reporting information for various types of dissemination activities

Type	**Conference, publication, specific presentation etc.**
Place	Which event / where the dissemination activity took place
Date	Date of the dissemination activity
Participants	Audience types and numbers
Organizers	The responsible partner
Topics	A short description of the presented topics
Benefits - Actions	Description of any specific actions agreed as a follow-up
Resources	Indication of (links to) presentations, photographs from the event, other related material

For every news item, the information to be reported is as follows:

Table 17: Reporting information for news items

Title	**Title of the news item**
Description	The main text of the news item
Resources	Indication of (links to) presentations, photographs, or other relative

For measuring effectiveness of the on-line communication, the following metrics must be compiled on a six-month basis, by the responsible partner:

Table 18: Reporting information for website and social media

Website	Website statistics report
Social Media	Number of followers, number of discussions opened, number of tweets & posts

For each dissemination and communication activity, an indicative list of evaluation criteria is presented in the following. Most criteria are quantitative, to provide a clearer and more accurate evaluation.

- **NEMECYS website**: The number of visitors per day/ traffic to the website;
- **Search engine optimization (SEO)**: position of 'NEMECYS project' on various search engines;
- **Focus links**: The number of sites **SEO** linking to NEMECYS, the number of link exchanges;
- **Press releases**: Number of press releases and media coverage (number of media broadcasts);
- **Advertising material (project brochure, poster)**: frequency advertising material production, number of advertising material;
- **Public deliverables**: Number of public deliverables;
- **Scientific papers, articles, etc.**: Number of papers, articles in scientific journals or conferences, , impact of journal or conference;

- **Pages in social media (Twitter, LinkedIn, etc.)**: Number of pages, number of tweets, number of participants;
- **Other projects**: Level of collaboration with other projects, number and size of joint activities;
- **Involvement/Participation**: Number of contributions received;
- **Meetings and one-to-one contacts**: number of meetings and contacts, fulfillment of meeting goals;
- **Events (workshops & conferences)**: Number of participants, number of presentations, number of other activities (poster sessions, panels, and round tables), and feedback received based on feedback forms.

A list of target values for quantitative indicators for evaluating the dissemination impact of the project are as follows:

- Publish relevant findings in scientific conferences and in scientific journals, aiming for a target of **20+ refereed publications**, targeting events and journals listed in Annexes 11.3 and 11.4.
- Participate in **7+ conferences** on healthcare, cyber security by design and European conferences on security.
- Organise **3+ thematic workshops** and **1+ conference** to promote and enhance R&D outcomes.
- Arrange and participate in up to 24 networking and joint activities (including concertation meetings, stakeholder workshops, commission events, and other project events),

7.2 Risks & Issues related to Communication and Dissemination

The main risk related to the communication and dissemination side of the project is presented in the following table. This risk, as well as any other identified risk or potential issue related to communication and dissemination, will be monitored and mitigated by the project coordinator. However, WP5 Leader will also examine these risks on a regular basis and report any changes to the coordinator.

Table 19 Risks related to communication and dissemination

Risk statement	Level of impact	Mitigating measures
The expected impact of the dissemination and communication activities is not reached.	Critical	Continuously keep tracking of the above-mentioned indicators. Organise regular meetings with the partners setting list of actions/ responsibilities .and undertake timely measures in order to avoid inclinations of the targeted KPIs.

8 Acknowledgement of EU Funding

All NEMECYS partners willproduce communication materialusing the standard templates whenever appropriate, and ensuring that the following are included:

- NEMECYS logo: The NEMECYS logo can be used for all kinds of publications, templates and for the website.

Figure 7: NEMECYS logo for publications

- EU emblem including the text "Co-funded by the European Union" as per the following examples:

Figure 8: EU emblem

Any publication or communication material should include the following disclaimer: *"Co-Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them".*
Partners from the UK need to follow the UK Research and Innovation (UKRI) guidelines and include in their publication or communication material the following statement: *"This work was funded by UK Research and Innovation (UKRI) under the UK government's Horizon Europe funding guarantee [grant number 101094323]."* For collaborative projects which are part of EU-funded consortia, such as NEMECYS, it is needed to cite the EU project according to the EU requirements in addition to acknowledging the funding from UKRI.[2]

9 Roles & Responsibilities

To ensure that all project partners have a clear understanding of their communication and dissemination responsibilities, this section will outline the key roles. Each partner is responsible for undertaking dissemination activities within their networks and for communicating the project at all relevant events,

[2] UKRI branding, guidelines and logos are available at https://www.ukri.org/about-us/contact-us/brand-guidelines/.

which they attend. The individual communication and dissemination activities per partner are presented as follows.

SINTEF will play an active part in WP5. We will actively communicate project results and achievements, both through the dedicated dissemination and communication channels established for the projects, as well as through our already established channels and network of partners. SINTEF also aims to publish project results in high impact journals and high-quality conferences proceedings. In addition, we will take an active role in organizing, managing, and contributing to thematic workshops, networking events, stakeholder workshops, concertation meetings and other similar relevant events.

MODE will actively communicate relevant project activities, deliverables, and results through:

- Established distribution channels (Company's website and social media)
- (If applicable) through network of membership organizations (e.g. EIT Health, Norway Healthtech, etc.).
- (If applicable) relevant events/exhibitions/etc. we participate (e.g. eHelsekonferansen, MEDICA, etc.)

IBM Research – Israel will strive to communicate and disseminate project results both internally and externally. Internally we will focus on demonstrating privacy services in IBM Think, IBM's yearly conference with emphasis on security and privacy, having exposure to representatives from IBM's business units, sales, and services, as well as IBM's business partners and customers. Externally, IBM Research – Israel will seek to publish the project results in appropriate, high-quality, peer-reviewed workshops, conferences and journals focusing on privacy and security, such as ACM CCS, IEEE Symposium on Security and Privacy, and USENIX Security Symposium..

ATC as W5 "Dissemination, Exploitation and Outreach" Leader, will oversee the planning, execution, monitoring, and reporting of project communication and dissemination activities. Additionally, ATC will actively communicate project objectives and results through Big Data Value Association (BDVA), its network of partners and established distribution channels (Company's website, social media, newsletters).

MS will contribute to the dissemination by presenting the project and achieved outcomes in healthcare events and particularly the yearly meeting of the AVIS@ organization. This yearly meeting, that includes the 25 hospitals composing the Public Health network of the east region of Spain and ensures the assistance of government representatives, is a very popular, specific and collaborative event in which novel strategies regarding Healthcare IT are shared and has served as booster for common projects in the mentioned network.

OSR will proactively communicate and disseminate the NEMECYS's scopes, objectives and the results with a series of activities.

- Presenting in Conferences, Events and Exhibitions
- Presenting to IT and Cybersecurity department of OSR and GSD (Gruppo San Donato)
- Publishing in the social media channels of the Advanced Technologies in Health and Wellbeing and also Ospedale San Raffaele.
- Participation in scientific publication of articles and papers with other partners of the project

UOI will actively participate in various workshops and events related to cybersecurity in Healthcare IT systems to communicate and disseminate project outcomes and contribute to knowledge sharing. UOI's participation in these events will enable the project to reach a wider audience, including healthcare professionals, IT experts, and researchers, who are interested in cybersecurity in the healthcare sector. UOI will also publish the project outcomes in various academic journals and conference proceedings, ensuring that the research findings are accessible to a broader community.

ICS is an ICT SME and will focus on communication and dissemination activities targeting industry and commerce. Key channels will be the ICE website, associations such as NESSI (https://nessi.eu) and AIOTI (https://aioti.eu), and applied research and industry events.

UoS will communicate with its key channels for the purposes of knowledge acquisition to supplement the project's other consultation activities. In particular, UoS has key contacts in the local Southampton, Hampshire and Wessex medical sector, and these will be engaged as necessary for the purposes of consultation and dissemination. Further, UoS has representation in European bodies such as NESSI (https://nessi.eu/) and the BDVA (https://www.bdva.eu/), and these will be key dissemination channels. As a case in point, NEMECYS work has already influenced a work-in-progress NESSI position paper on software security. UoS also seeks to publish its results in academic journals and conferences (venues similar to those of other NEMECYS partners), and will actively collaborate with other NEMECYS partners in joint publications. Finally UoS has an ongoing initative to open source its cybersecurity risk management tool (System Security Modeller – SSM) under the branding "SPYDERISK" and is currently negotiating partnerships with an existing & influential cybersecurity open source project to bring the SSM into it. NEMECYS results will be feeding into this channel for both dissemination and as a route to exploitation.

ICE is an ICT SME and will focus on communication and dissemination activities targeting industry and commerce. Key channels will be the ICE website, associations such as NESSI (https://nessi.eu) and AIOTI (https://aioti.eu), and applied research and industry events.

PDN will actively communicate and disseminate relevant project activities, deliverables, and results through:

- Established distribution channels (Company's website and social media)
- Events organized by PD Neurotechnology (PDMonitor Training Days, Medical Advisory Board Meetings)

- Relevant events/exhibitions/etc. PD Neurotechnology may participate
- Our consultants on medical device affairs which are in contact with other medical device manufacturers and can communicate/disseminate NEMECYS outcomes.

10 Conclusions

This deliverable is part of WP5 "Dissemination, Exploitation and Outreach" and provides information regarding NEMECYS's dissemination and communication plan. The report presents an overview of the targeted audiences and identifies the tactics to be used in order to communicate and disseminate the project's activities and results. NEMECYS partners have indicated an extensive list of stakeholders' associations, related organisations and networks that are already in contact in Annex 11.1. This list will be revisited and updated with other related to NEMECYS project objectives organisations through the project lifetime. Regular communication with the indicated bodies will enhance the communication and will allow the dissemination of the project activities and outcomes to the targeted audiences. Relevant scientific events and journals that are likely to be suitable for presenting the project research activities and promoting its goals are listed in Annexes 11.3 and 11.4. These lists will be updated and enriched during the project lifetime. EU research projects and initiatives related to NEMECYS are identified and presented in Annex 11.4. NEMECYS project will combine forces with these initiatives in order achieve broader audience and enhance the impact of the planned dissemination and communication activities. . The variety of expertise, competences and the dedication of the NEMECYS partners guarantees the effectiveness and maximises the expectations of the planned dissemination and communication activities

11 Annexes

11.1 Annex: Target stakeholder groups

Relevant Community/ Organisation/ Industry Body/ Regulatory Body/Advisory Group	Who	Type of relationship: member/partner/affiliate/ other
AdvaMed - Advanced Medical Technology Association - https://www.advamed.org/	EAB	Active membership participation.
AIOTI https://aioti.eu/	ICE	Active membership participation.
AISP - Association of Information Security Professionals - https://www.aisp.sg/	EAB	Active membership participation.
Aleap https://www.aleap.no/	MODE	Active membership participation
Big Data Value Association (BDVA) www.bdva.eu	ATC, SINTEF	Board of Directors
CCAPAC - Cybersecurity Coalition for Asia Pacific - https://www.accesspartnership.com/ cybersecurity-policy-for-operational-technology-a-guide-for-governments/	EAB	Active membership participation.
DNV https://www.dnv.com/assurance/healthcare/index.html	SINTEF	
DSAC - Domestic Security Alliance Council - https://www.dsac.gov/	EAB	Active membership participation.
ECSO https://www.ecs-org.eu/	SINTEF	Active membership participation.
EIT Health https://eithealth.eu/who-we-are/	MODE	Other – Alumni
ENISA https://www.enisa.europa.eu/	SINTEF	Specific contacts, critical infrastructure protection
Gruppo San Donato https://www.grupposandonato.it/	OSR	Italy's largest private health group, one of the largest in Europe, >4.7M patients/year
Healthcare informatics association of Valencia Community (http://www.avisados.org/)	MS	Active membership participation.
Healthcare Information and Management Systems Society (https://www.himss.org/)	MS	CIO of MS is a member of the evaluation group of HIMSS, a global thought leader
H-ISAC - Health Information Sharing and Analysis Center - https://h-isac.org/	EAB	Active membership participation.
HSCC International Task Group - Healthcare and Public Health Sector Joint Cybersecurity Working Group - https://healthsectorcouncil.org/	EAB	Active membership participation.
IMDRF - International Medical Device Regulators Forum - http://www.imdrf.org/	EAB	Active membership participation.
MDIC - Medical Device Innovation Consortium - https://mdic.org/	EAB	Active membership participation.

MTE - MedTech Europe - https://www.medtecheurope.org/	EAB	Active membership participation.
Networked European Software and Services Initiative (NESSI) https://www.nessi.eu	UoS, ICE, ATC, SINTEF	Partners
Norway Health Tech https://www.norwayhealthtech.com/	MODE	Active membership participation
Norwegian ethics committee	MODE	Ethical evaluation & approval of research projects
Norwegian Medicines Agency http://noma.no	MODE	Other
NSSC – Norwegian Smart Care Cluster https://www.smartcarecluster.no/	MODE	Active membership participation
U.S. FBI InfraGard Health Care Working Group - https://www.infragard.org/	EAB	Active membership participation.
UK National Cyber Security Centre (NCSC) https://www.ncsc.gov.uk/	UoS	Hosts an interdisciplinary GCHQ Academic Centre of Excellence in Cybersecurity Research and a Cybersecurity Academy, both linked to industry, the cybersecurity community and the NCSC
UK National Institute for Health Research https://www.nihr.ac.uk/	UoS	Engagement in a "Social Data Foundation" Trusted Research Environment where multistakeholder medical data may be securely analysed
DARE UK https://dareuk.org.uk/ DARE UK (Data and Analytics Research Environments UK) is a programme funded by UK Research and Innovation (UKRI) to design and deliver coordinated and trustworthy national data research infrastructure to support cross-domain research for public good.	UoS	Project Contributor
PETRAS-IoT https://petras-iot.org/ The PETRAS National Centre of Excellence exists to ensure that technological advances in the Internet of Things (IoT) are developed and applied in consumer and business contexts, safely and securely.	UoS	Project Contributor
The UKRI Trustworthy Autonomous Systems (TAS) Hub https://tas.ac.uk/ The TAS Hub enables the development of socially beneficial autonomous systems that are both trustworthy in principle and trusted in practice by the public, government, and industry. The TAS Hub assembles a team from the Universities of Southampton, Nottingham and King's College London. The Hub sits at the centre of the £33M Trustworthy Autonomous Systems Programme, funded by the UKRI Strategic Priorities Fund.	UoS	Partner

NHS England - Transformation Directorate https://transform.england.nhs.uk/ supports transformation to improve health and care for everyone.	UoS	Contact

11.2 Annex: List of possible venues

Conference	Location	Dates	URL	Submission deadline	Proceedings publisher	Proceedings series
5th Workshop on Internet of Things Security and Privacy (WISP)	Berlin		https://globaliotsummit.org/workshops-2023/	April 2nd 2023	Springer	LNCS
Cyber Science	Copenhagen, Denmark	3-4 Jul., 2023	http://cyber-conference.eu	April 7th 2023	Springer	Proceedings in Complexity
IEEE ICTS4eHealth 2023 - International Conference on ICT solutions for eHealth	Tunis, Tunisia	9-12, Jul., 2023	https://icts4ehealth.icar.cnr.it	April 16 2023	IEEE	
International Conference on Health and Social Care Information Systems and Technologies	Porto, Portugal	8-10 Nov. 2023	http://hcist.scika.org/	April 17 2023	Elsevier	Procedia Computer Science
30th ACM Conference on Computer and Communications Security	Copenhagen, Denmark	26-30 Nov., 2023	https://www.sigsac.org/ccs/CCS2023/index.html	May 4, 2023	ACM	Proceedings in the ACM Digital Library
Annual Computer Security Applications Conference	Austin, Texas	4-8 Dec. 2023	https://www.acsac.org/	May 22, 2023	ACM	Proceedings in the ACM Digital Library
IEEE Secure Development Conference	Atlanta, Georgia, USA	Oct. 18-20 2023	https://secdev.ieee.org/	June 2, 2023	IEEE	IEEE Proceedings

IEEE Healthcom	Chongqing, China	15-17 December 2023	https://ieee-healthcom.org	July 15	IEEE	IEEE Proceedings
SecAssure@ESORICS	The Hague, Netherlands	September 25-29 2023	https://www.ntnu.edu/secassure	July 10	Springer	LNCS
Nordsec	Oslo, Norway	November 16-17 2023	http://nordsec.org/	August 1st	Springer	LNCS
SecHealth @ARES	Benevento, Italy	August 29 - September 01, 2023	https://www.ares-conference.eu/workshops/sechealth-2023/	May 8 2023	ACM	Proceedings in the ACM Digital Library

In addition annual events such as IEEE Symposium on Security and Privacy and USENIX Security Symposium will be followed by the NEMECYS partners.

11.3 Annex: Relevant refereed journals

Journal	Publisher	URL
Computers & Security	Elsevier	https://www.sciencedirect.com/journal/computers-and-security
Journal of Cybersecurity	Oxford University Press	https://academic.oup.com/cybersecurity

11.4 Annex: Existing EU initiatives

Name	Description	Contact / URL
CybAlliance	The International Alliance for Strengthening Cybersecurity and Privacy in Healthcare (CybAlliance)	The Norwegian Computing Center. https://nr.no/en/projects/kompetanseheving-for-okt-digital-sikkerhet-i-helsevesenet/
CYCLOMED	"Sibling" project funded under the HORIZON-HLTH-2022-IND-13-01 topic. Coordinated by CHARITE (DE)	https://www.cylcomed.eu/
ENTRUST	"Sibling" project funded under the HORIZON-HLTH-2022-IND-13-01 topic. Coordinated by UNISYSTEMS LUXEMBOURG SARL (LU)	https://www.entrust-he.eu/

MEDSECURANCE	"Sibling" project funded under the HORIZON-HLTH-2022-IND-13-01 topic. Coordinated by UNPARALLEL INNOVATION LDA (PT)	Webpage not yet available
NESIOT	Norwegian Ecosystem for Secure IT-OT Integration (NESIOT) brings together multiple stakeholders such as sensor/devices manufacturers, telecom operators, cloud and data analysis solution providers, industrial system operators etc., and to exploit enabling technologies and the secure application of those technologies.	https://www.ntnu.edu/norcics/it-ot-integration-nesiot
NORCICS	Center for Research-based Innovation (SFI) Norwegian Center for Cybersecurity in Critical Sectors (NORCICS)	https://www.ntnu.edu/norcics
ORSHIN	ORSHIN: Open-source ReSilient Hardware and software for Internet of thiNgs. How to design embedded and connected devices taking advantage of open-source hardware (and software)	https://horizon-orshin.eu/
SEPTON	"Sibling" project funded under the HORIZON-HLTH-2022-IND-13-01 topic. Coordinated by SPACE HELLAS SA (EL)	Webpage not yet available