HORIZON-HLTH-2022-IND-13-01

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

NEMECYS
New Medical Cybersecurity and design Solutions

D5.3 Report on Dissemination and Communication Activities (first)

Project Reference No	NEMECYS – 101094323
Deliverable	D5.3 Report on Dissemination and Communication Activities (first)
Work package	WP5: Dissemination, Exploitation and Outreach
Type	R - Document, report
Dissemination Level	PU - Public (fully open)
Date	30/06/2024
Status	Final v1.0
Editor	George Zissis (ATC)
Contributor	Karin Bernsmed (SINTEF)
Reviewers	Line Thompson (SINTEF), Tonny Velin (ICE), Paula Gomez Peidro (RS)
Document description	This deliverable reports the accomplished dissemination and communication activities of NEMECYS for the first 18 months of the project.

Disclaimer

The NEMECYS project is co-funded by the European Union under grant agreement ID 101094323, by UK Research and Innovation (UKRI) under the UK government's Horizon Europe funding guarantee grant numbers 10065802, 10050933 and 10061304, and by the Swiss State Secretariat for Education, Research and Innovation (SERI).

Document revision history

Version	Date	Modifications introduced	
		Modification reason	Modified by
v0.1	24/04/2024	TOC	George Zissis
v0.2	22/05/2024	Sections 2,3,4,5	George Zissis
v0.3	31/05/2024	Sections 6.1.1, 6.1.2	All project partners
v0.4	20/06/2024	1st complete draft	George Zissis
v0.5	28/06/2024	Reviewed by SINTEF, ICE, RSH	Line Thompson, Tonny Velin, Paula Gomez Peidro
v0.9	29/06/2024	Final draft for review by SINTEF	George Zissis (ATC)
v1.0	30/06/2024	Final version	Karin Bernsmed (SINTEF)

Executive summary

During its initial 18-month phase, NEMECYS achieved significant milestones in disseminating its research findings and engaging stakeholders across Europe. The project successfully published several scientific articles, contributing valuable insights to the cybersecurity landscape of medical devices.

NEMECYS hosted 4 workshops in Spain, Italy, Greece, and Norway, gathering stakeholders to discuss emerging challenges on cybersecurity regulations, standards, and best practices and collaborate on solutions in this domain. A key workshop in Brussels on July 6, 2023, convened participants from NEMECYS' sibling projects funded under the same call, fostering productive exchanges and joint initiatives.

The project actively participated in multiple scientific conferences and engaged in various events such as conferences, workshops, and stakeholder meetings. These activities not only increased NEMECYS' visibility in the scientific, research and industrial arena but also facilitated knowledge sharing and alignment with industry standards.

Furthermore, NEMECYS strategically enhanced its network by joining the European Cluster for Securing Critical Infrastructures (ECSCI), enabling broader collaboration and synergies with other EU-funded projects focused on cybersecurity.

Online visibility efforts through its website, LinkedIn, and Twitter channels have expanded NEMECYS' outreach within the cybersecurity and medical device sectors, reinforcing its role as a leading contributor to enhancing security standards for connected medical devices.

In summary, NEMECYS' dissemination efforts during this period have been instrumental in advancing research impact, fostering collaborative partnerships, and advocating for robust cybersecurity measures in healthcare technology.

Table of contents

List of figures

List of tables

List of abbreviations

Abbreviation	Definition
ACM	Association for Computing Machinery
CMD	Connected Medical Device
CRA	Cyber Resilience Act
EAB	External Advisory Board
EU	European Union
HADEA	European Health and Digital Executive Agency
MD	Medical Device
MDCG	Medical Device Coordination Group
MDR	Medical Device Regulation
R&D	Research and Development
SBOM	Software Bill of Materials
ECSCI	European Cluster for Securing Critical Infrastructures

1 Introduction

The NEMECYS project aims to enhance the cybersecurity of connected medical devices (CMDs) by developing new assessment techniques and tools. This initiative supports device manufacturers, integrators, and healthcare providers to ensure security-by-design, enabling personalized, distributed, and home-based healthcare services. By providing best practice guidelines, risk-benefit schemes, and compliance tools, NEMECYS ensures CMDs are both secure and effective in improving patient care and quality of life.

The main objectives of the NEMECYS project are to review and enhance Medical Device (MD) guidelines by consulting domain experts and conducting four case studies to identify gaps and best practices for Connected Medical Devices (CMDs). The project also aims to develop risk-benefit schemes and cybersecurity risk assessment tools tailored for CMDs. Additionally, NEMECYS will provide tools and toolboxes for CMD Manufacturers at design time, CMD System Integrators during integration, and Operators like hospitals or care providers during the operation of CMDs in connected scenarios.

In this context, Work Package 5 (WP5) aims at engaging with key stakeholders and disseminating the results of the NEMECYS project. This will involve large-scale dissemination and communication activities, both online and offline, to raise awareness among scientific communities, medical device industry stakeholders, and cybersecurity experts. By creating awareness of the project, WP5 seeks to engage these groups in project activities such as consultations, demonstrations, and user trials, ensuring their active participation and feedback.

In this framework, a dissemination and communication strategy (D5.1 Dissemination & Communication Plan) appropriate for the nature and needs of the project was designed early in the project's lifecycle. Based on this strategy, NEMECYS—over the first 18 months—has carried out traditional, large-scale dissemination and communication activities, through both online and offline channels.

1.1 Purpose and scope

This report describes the dissemination and communication activities conducted during the first 18 months of the NEMECYS project and outlines the planned activities for the remaining duration of the project. Specifically, it details the dissemination and communication objectives and strategies for the reporting period, and presents the tools and activities undertaken to achieve the set objectives, disseminate the project, and implement the strategy as outlined in deliverable D5.1 Dissemination & Communication Plan.

1.2 Structure of the deliverable and methodology

1.2.1 Structure of the deliverable

The deliverable outlines a comprehensive overview of the dissemination and communication efforts undertaken during the initial 18 months of the project. It begins with an introduction detailing the purpose and scope, followed by an explanation of the methodology and structure of the report. A summary of the dissemination and communication plan provides a strategic framework. The report then covers brand identity and project materials, including the project logo, brand manual, templates, presentation materials, and infographics. It also discusses the development and analytics of the project website, content creation such as blog posts and video series, and the management of social media channels. Detailed sections on dissemination activities, including scientific publications, event participation, workshops, collaborations, clustering activities, and the formation of an External Advisory Board (EAB), are presented. The report concludes with an assessment of the impact of dissemination and communication efforts and outlines future plans for the project.

1.2.2 Summary of the dissemination and communication plan

The NEMECYS project has outlined various channels and methods to ensure effective dissemination and communication of its achievements and results to target stakeholder groups across both online and offline platforms. Key dissemination activities include scientific publications, participation in conferences and events, conducting workshops, organizing a final conference, and engaging with existing EU initiatives.

Communication efforts primarily involve maintaining a project website and utilizing social media platforms. The primary stakeholders targeted by the project include CMD manufacturers, suppliers, integrators, healthcare providers, operators, advisory bodies like the MDCG, notified bodies, regulators, cybersecurity experts from diverse domains, and professionals from sectors where IoT devices handle sensitive data. Additionally, the project's outcomes are relevant to a broader audience including patients, the general public, and society at large.

The NEMECYS dissemination & communication strategy unfolds across three periods spanning Year 1 to Year 3:

- The ***awareness-oriented period*** aims to raise stakeholder awareness and public interest. Activities include developing a dissemination plan, creating a public website, designing project materials (such as posters and leaflets), and conducting introductory presentations and workshops. This period aligns with the first year of the project.
  During the awareness-oriented period (M1-M12), NEMECYS focused on establishing its brand and disseminating project goals through strategic messaging, essential dissemination materials, and the launch of NEMECYS website and social media profiles. Stakeholder engagement is fostered through international presentations and collaborations with related projects and cybersecurity communities specializing in CMDs.

- The ***result-oriented period*** focuses on promoting project results to interested parties, particularly the scientific community. It involves publishing public deliverables and news on the project website, submitting high-quality papers to scientific journals, delivering presentations at conferences and workshops, issuing press releases, and updating social media channels. This period continues through the second year.
  In Period 2 (M12-M24), the result-oriented period, NEMECYS aims to expand stakeholder participation and engage a wider community. Activities include involving stakeholders in disseminating project outcomes, establishing social media communities, ensuring active feedback, and collaborating with cybersecurity projects focused on CMDs. This period includes organizing thematic events, preparing publications for conferences and journals, issuing press releases, conducting workshops, and presenting findings at relevant forums.

- The ***sustainability and wider dissemination period*** aims to ensure the longevity of project outcomes. Activities include developing a sustainability plan, defining pathways for future communication and evolution of results among NEMECYS partners and stakeholders, and engaging CMD manufacturers, integrators, operators, and regulatory authorities. This period spans the third year of the project.
  During Period 3 (M24-M36), the sustainability and wider dissemination period, NEMECYS focuses on disseminating final project activities and outcomes. This includes updating the project website, issuing multiple press releases, producing articles and presentations, preparing publications for international conferences and journals, organizing thematic events, and maintaining communication through social media, workshops, and publications. Efforts are made to sustain communication within the NEMECYS cybersecurity community beyond the project's duration.

During the first 18 months of the NEMECYS project, dissemination and communication activities adhered closely to the outlined strategy, aimed at raising awareness and engaging stakeholders effectively.

2 Brand identity & project materials

We need to ensure that everyone who interacts with the project, will experience a consistent and unified image, hence, we formulated a brand kit, also sometimes called a brand identity kit, operating like a toolbox for the project's visual identity. It contains the essential elements that make the project recognizable and consistent across different platforms, such as:

- The logo and the corresponding colour palette
- Brand manual, i.e. a separate document that sums up all the appropriate brand guidelines, i.e how to use existing visual elements.

2.1.1 Document template

Document templates offer similar advantages to PowerPoint templates, but with some key differences, such as focusing on

- Standardization and consistency, since they ensure that all documents follow the same format, structure, and terminology;
- Efficiency, since pre-defined sections and formatting save time and effort for the team members, who wouldn't need to build documents from scratch;
- Collaboration and version control, making it easier for all collaborating participants to track changes and identify the latest version of a document.

For that matter, we delivered a variety of MS Word (doc) templates to cover multiple needs of the team, such as deliverables and reports, meeting minutes, agenda and more.

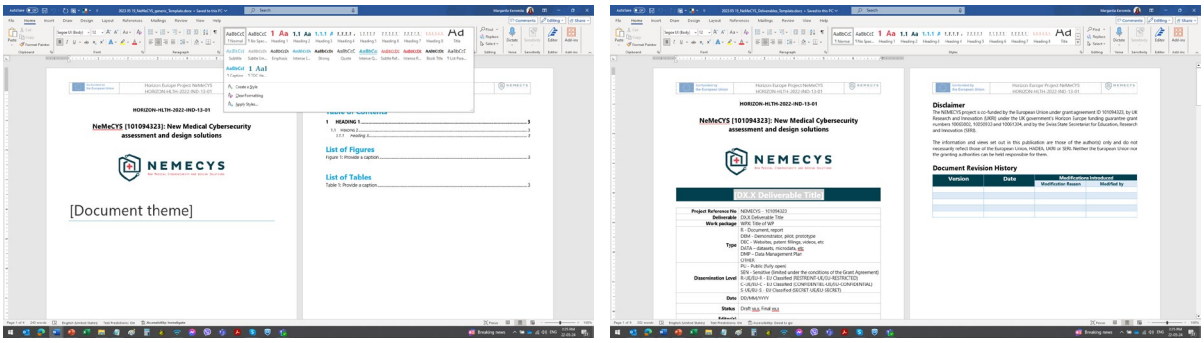


Figure 1: NEMECYS Word template.

2.2 Project logo

The project logo was the first branding element created early on since it was the key asset that would drive all the visual identity of the project. In terms of depiction, it consists 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.

NEMECYS
NEW MEDICAL CYBERSECURITY AND DESIGN SOLUTIONS

Figure 2: The NEMECYS project logo.

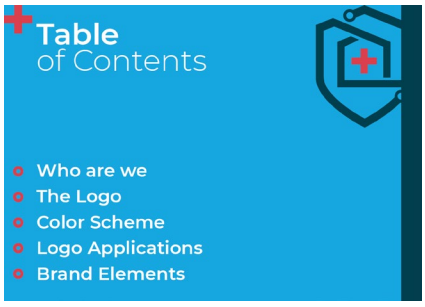
The colour palette applied consists of *(i)* a tone of blue (Iris Blue), the typical colour used in healthcare for its ability, attested by colour psychology, to normalize the heartbeat frequency and blood pressure, and to remove the sense of anxiety; *(ii)* and a tone of yellow (Ronchi), symbol of sunlight but also of knowledge and energy (see Figure 2).

Figure 3: NEMECYS chromatic palette and font.

2.3 Brand manual

The brand manual is a distinct document, that covers things like:

- Logo usage rules
- Minimum size requirements for the logo
- Typography, i.e. how fonts should be applied in different contexts (print vs. web, communication collaterals or templates), including headings, body text, and any other variations.
- Imagery, i.e. examples of the types of images that best represent the project's style and tone



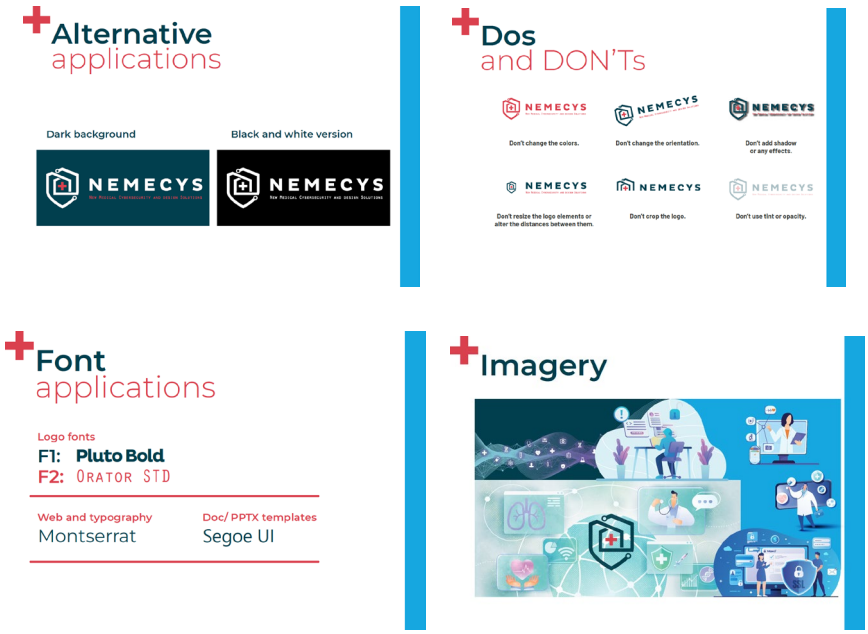


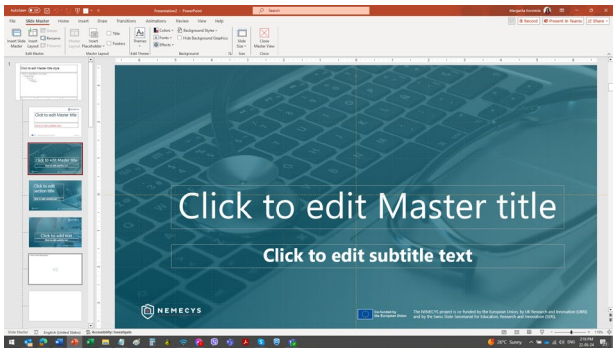
Figure 4: NEMECYS brand manual.

2.4 Project templates

2.4.1 Presentation template

In order to ensure a consistent look and feel for all project presentations, saving time and effort in formatting, we delivered a rich MS PowerPoint (pptx) template, with pre-defined layouts, fonts, and colour schemes that can streamline the presentation creation process and help structure presentations in a way that promotes clear and concise communication.

By having a template handling the visual aspects, the consortium team members can focus their energy on the content itself - the findings, methodology, and conclusions. The template incorporates the project's branding elements, creating a professional and unified presentation for stakeholders.



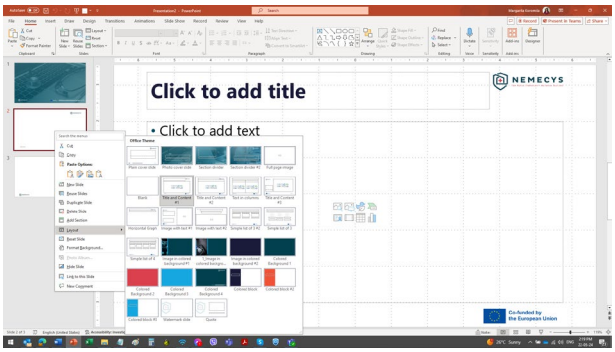


Figure 5: NEMECYS PowerPoint template.

2.5 Project presentation

Following the above-mentioned template, the team created an introductory PowerPoint presentation, 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.

Figure 6: The title slide of the introductory presentation of the NEMECYS project.

2.6 Project infographics

In an effort to support the stakeholder engagement process and help targeted audiences to easily grasp what the project is about, we created an infographic that can be either sent via email communications or shared via the project's website and social media accounts.

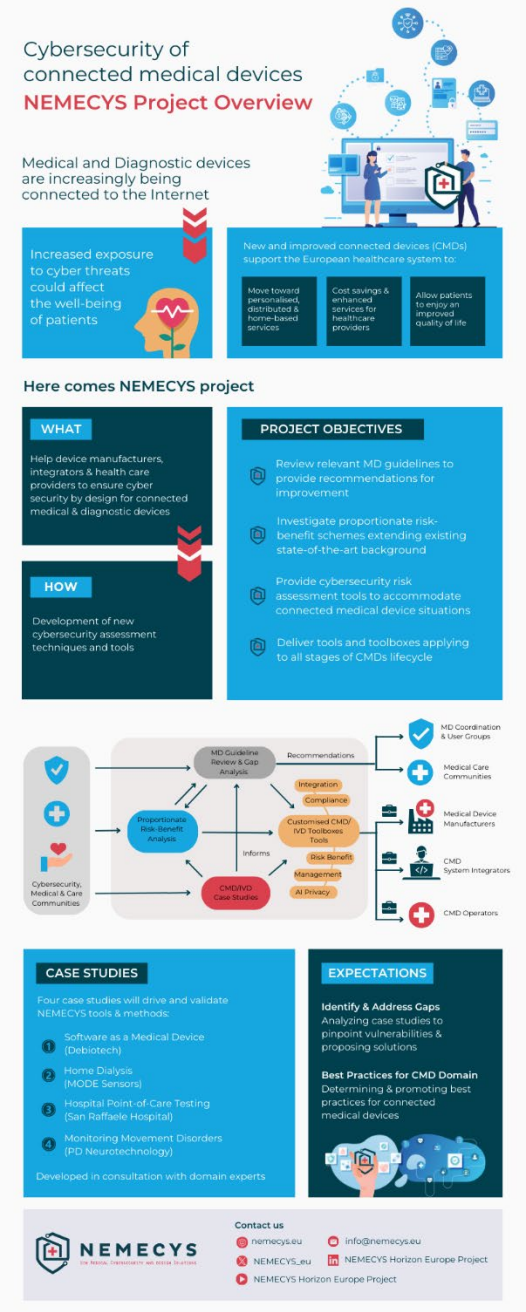


Figure 7: NEMECYS overview infographic.

2.7 Project poster

In order for the project team to be able to communicate the project's goals, achievements, and impact while attending meetings and events, A0 posters are widely used.

Up to now, we have created 1 poster, prominently featuring details on the project's field, scope and aspirations, basic contact details and of course, specific funding program details associated with the project.

Figure 8: NEMECYS poster.

3 Project website

3.1 Website overview

A strong online presence clearly supports the visibility of the project and easy access to related information and work done for multiple audiences. The NEMECYS website was officially released during the spring of 2023 under the https://nemecys.eu/ domain.

Figure 9: NEMECYS web site (home page).

3.2 Website analytics

The metrics in Table 1 provide insights into the website's performance and user engagement, highlighting the reach and effectiveness of NEMECYS's online presence.

Table 1: List NEMECYS web site analytics (launch to June 2024).

Users	526
New Users	524
Returning Users	85
Avg Engagement Time	0m 43 sec
Engaged Sessions	379
Engagement Rate	47.55%
Pageviews	1364

4 Content development

4.1 Blog posts

By implementing a well-defined content marketing strategy with informative and engaging blog posts, NEMECYS project can achieve greater transparency, public engagement, and ultimately, maximize the impact of the work done for the benefit of Europe and beyond.
In fact, blog posts can explain the project's goals, methodology, and progress, keeping stakeholders informed and promoting accountability. Moreover, blog posts can explain complex topics in a clear and engaging way, fostering public interest in science and innovation funded by the EU.

That is the basic axes the team followed when creating 2 articles closely related to the project's domain:

- The Challenges And Opportunities Of Medical Device Cybersecurity (available at https://nemecys.eu/the-challenges-and-opportunities-of-medical-device-cybersecurity/)
- Cybersecurity In The Era Of Medical Internet Of Things (IoT) (available at Cybersecurity in the era of Medical Internet of Things (IoT) – Nemecys)

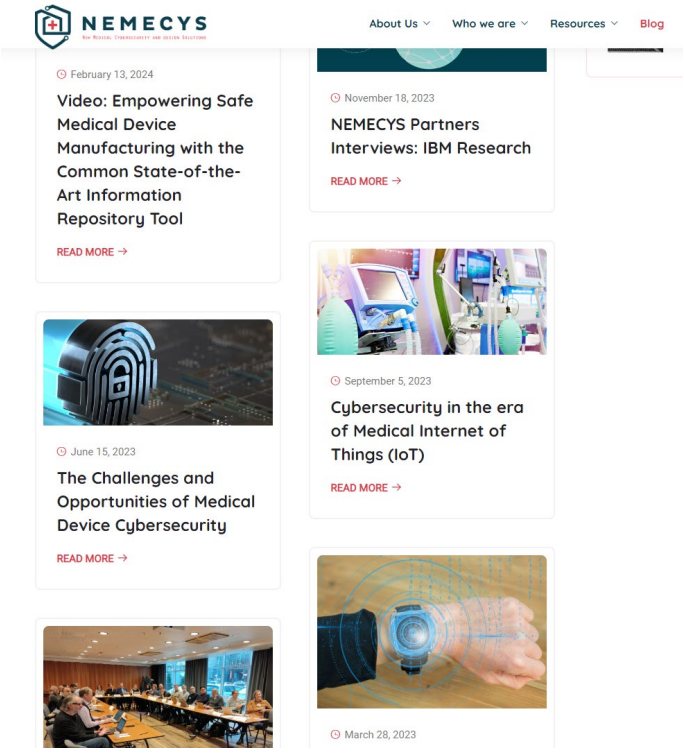


Figure 10: NEMECYS blog section (1).

In addition, blog posts can be used to reach a wider audience and thus maximize the NEMECYS impact. Sharing updates to keep stakeholders informed about the project's progress, milestones achieved, and

upcoming activities, project findings and innovations in the next months, can spark discussions, answer questions, and build a community around the project's goals and achievements.

Finally, partner spotlights are another crucial editorial aspect. Featuring blog posts highlighting the contributions of different partners involved in the project, showcasing collaboration and expertise, establish the project team's expertise and build trust among stakeholders. For that matter, apart from creating the "Consortium Video Series" (see details below), we have also added those assets to the web site.

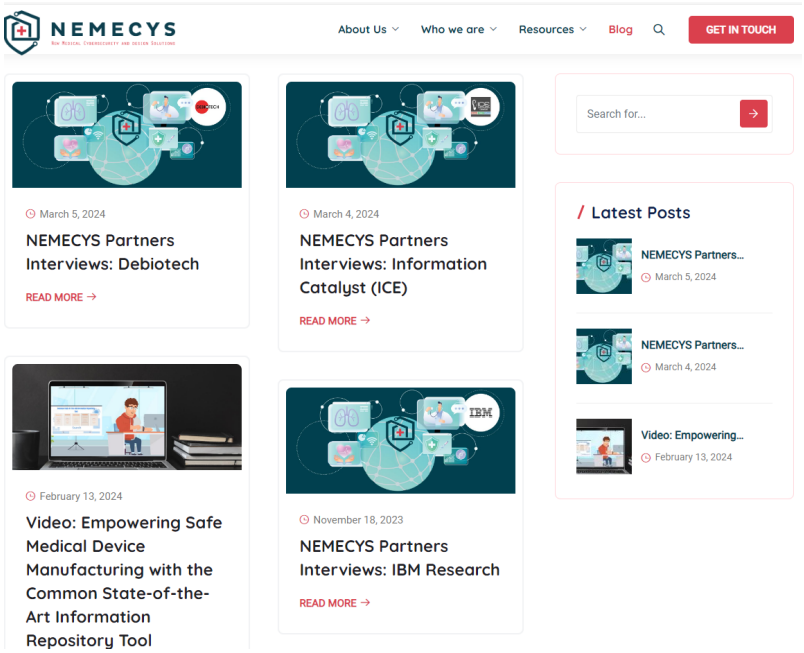


Figure 11: NEMECYS blog section (2).

4.2 Consortium video series

In order to stress the transparency and accountability aspects of our work, we have decided to create videos featuring project partners explain how each partner contributes, showcasing the collaborative nature of the project and justifying the involvement of multiple entities.

Up to now[1], we have created and published 3 of them, that also serve as communication tools for the project. By showcasing partner involvement, we aim to raise awareness about the project's goals and reach a wider audience. This can attract potential collaborators or beneficiaries. Highlighting partner contributions also demonstrates the project's impact across different domains.

[1] The official due date of the deliverable "D5.3 Dissemination Communication Report" is at M18: June 30th, 2024.

All videos are accessible via the NEMECYS YouTube channel and are also referenced within the project's web site (Blog section).

Moreover, the video creation process itself can foster collaboration among partners. Working together to develop a clear message strengthens communication and understanding of each other's roles. Partners can also leverage the videos on their own channels, further expanding the project's reach and promoting collaboration within the broader ecosystem.

5 Social media channels

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 α YouTube Channel, all promoted via the NEMECYS web page. 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 are also published, using a list of relevant hashtags.

5.1 LinkedIn

A LinkedIn page[2] 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 set in D5.1, and are interested in relevant issues, to share news, discussion and related content. This profile is the project's primary social media channel.

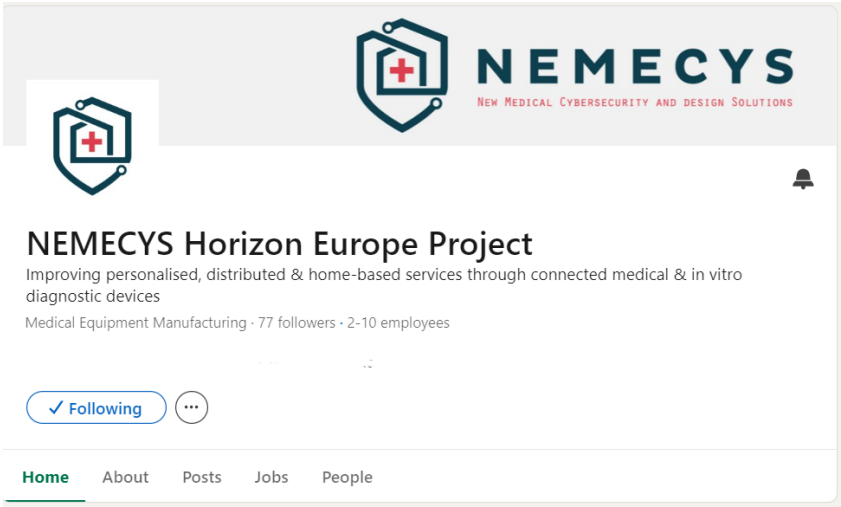


Figure 12: NEMECYS LinkedIn Page.

Project members are encouraged to actively use their own LinkedIn profiles to build the NEMECYS community on LinkedIn. Moreover, the content feed from this account is also accessible via the footer of the NEMECYS website.

[2] https://www.linkedin.com/company/nemecys-horizon-eu-project

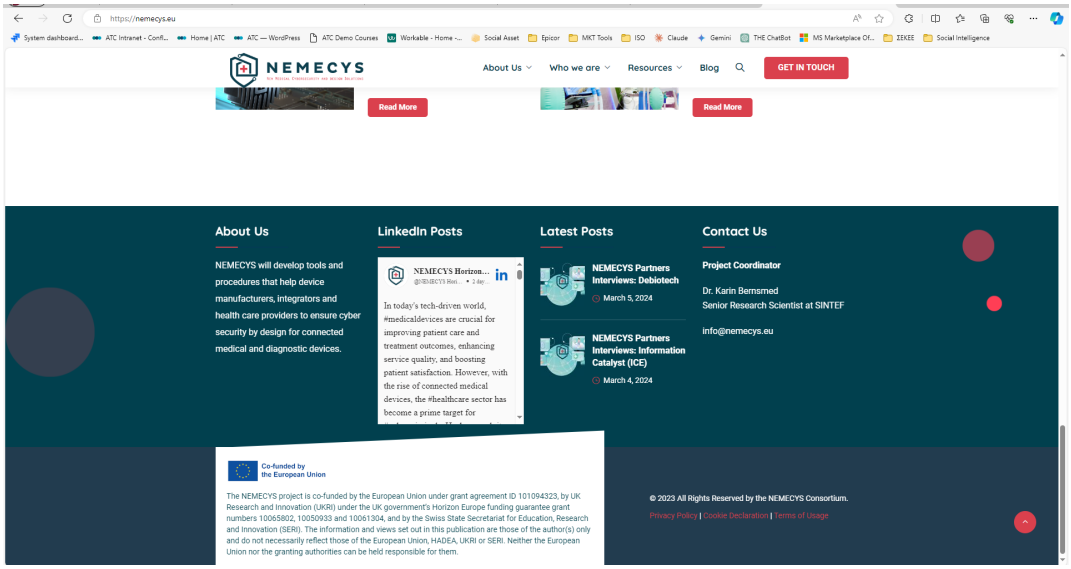


Figure 13: NEMECYS web site (LinkedIn feed).

Here are some key performance highlights (performance KPIs) of the NEMECYS LinkedIn page from project launch till June 2024.

Table 2: NEMECYS LinkedIn profile KPIs (launch to June 2024).

Followers	83
Reach	3825
Number of posts	34
Clicks	150
Likes	118
Reposts	36
Engagement Rate	6,62%

5.2 Twitter/X

The Twitter/X account " NEMECYS_EU"[3] has been created and it is being used to provide short news updates and other tweets about the project. The respective account will be secondary channel in support of the website and LinkedIn presence, which will be exploited by all partners.

[3] https://x.com/NEMECYS_eu

Figure 14: NEMECYS Twitter account.

Here are some key performance highlights (performance KPIs) of the NEMECYS Twitter/X account from project launch till June 2024.

Table 3: NEMECYS Twitter/X account KPIs (launch to June 2024).

Followers	48
Reach	941
Number of posts	52
Clicks	3
Likes	64
Reposts	19
Engagement Rate	5%

5.3 YouTube

The YouTube channel[4] of the NEMECYS project was established to serve as a repository for demo videos created by the project partners. This platform facilitates the easy sharing and distribution of these videos across various social media channels, websites, and other digital platforms. Through this channel,

[4] https://www.youtube.com/@NEMECYS_eu

NEMECYS aims to enhance its outreach and engagement by visually demonstrating its advancements and contributions in cybersecurity and medical device sectors.

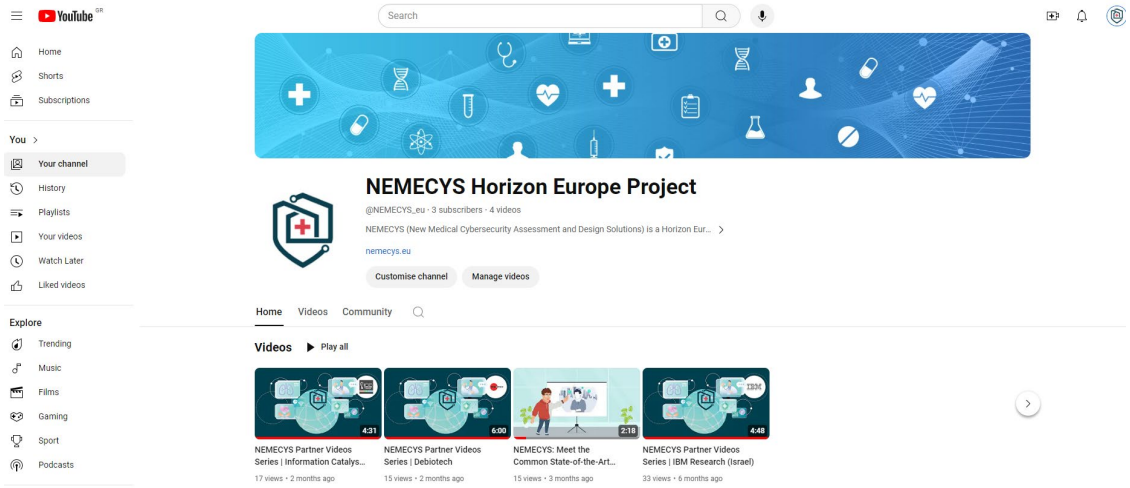


Figure 15: NEMECYS YouTube Channel.

Here are some key performance highlights (performance KPIs) of the NEMECYS YouTube Channel from project launch till June 2024.

Table 4: NEMECYS YouTube channel KPIs (launch to June 2024)

Subscribers	3
Views	85
Number of videos	4
Avg view duration	0:51
How viewers find our videos	linkedin.com, nemecys.eu
Impressions	425

5.4 Build relations with stakeholders

Social media offers a powerful platform to connect and build relationships with the various stakeholders within our ecosystem. Hence, early on, we made sure to map out the different stakeholders within the NEMECYS ecosystem, including partners projects, organizations, influencers, thought leaders and more.

Table 5: List of key stakeholders to monitor and engage.

1	European Cyber Security Organisation (ECSO)
2	BDVA - Big Data Value Association
3	DNV
4	AdvaMed
5	European Union Agency for Cybersecurity (ENISA)
6	Medical Device Innovation Consortium (MDIC)
7	Health Sector Coordinating Council - Cybersecurity
8	NHS Transformation Directorate
9	NIHR (National Institute for Health and Care Research)
10	National Cyber Security Centre
11	Norwegian Smart Care Cluster
12	Medical Device Network
13	Norway Health Tech
14	EIT Health
15	Health-ISAC

Moreover, we now follow relevant hashtags, participate in discussions, and share valuable insights, when possible. We also tend to tag relevant stakeholders in our posts to increase visibility and build connections.

6 Dissemination and communication activities

6.1 Dissemination activities

6.1.1 Scientific publications

Partner(s)	Type of publication	DOI/Link	Title	Main author	Title of the periodical or the series	Publisher	Publication year
SINTEF	Conference paper	Not yet available (accepted)	Fuzzing the ARM Cortex-M: A Survey	Silje Marie Sørlien	Cyber Science 2024	Springer	2024
SINTEF	Conference paper	Not yet available (accepted)	Workshop Insights: Navigating Cybersecurity Regulations for Device Manufacturers and Healthcare Operators	Andrea N. Skytterholm	Cyber Science 2024	Springer	2024
SINTEF	Conference paper	https://doi.org/10.1145/3655693.3661297	Security-by-design challenges for medical device manufacturers	Karin Bernsmed	Proceedings of the 2024 European Inter-disciplinary Cybersecurity Conference (EICC '24)	ACM	2024

Partner(s)	Type of publication	DOI/Link	Title	Main author	Title of the periodical or the series	Publisher	Publication year
IBM	Book chapter	https://shop.elsevier.com/books/ethics-in-online-ai-based-systems/caballe/978-0-443-18851-0	Assessing and Implementing Trustworthy AI Across Multiple Dimensions	Abigail Goldsteen	Ethics in Online AI-Based Systems: Risks and Opportunities in Current Technological Trends	Elsevier	2024
IBM	Conference paper	https://doi.org/10.48550/arXiv.2310.07219	Improving Membership Inference Attacks against Classification Models	Shlomit Shachor	IDT-24	Springer	2024
SINTEF, UOS, ICE, IBM, MS, UOI	Conference paper	https://www.sintef.no/en/publications/publication/2205604/	NEMECYS: Addressing Challenges to Building Security Into Connected Medical Devices	Martin Gilje Jaatun	HCist - International Conference on Health and Social Care Information Systems and Technologies 2023	Elsevier	2024

Partner(s)	Type of publication	DOI/Link	Title	Main author	Title of the periodical or the series	Publisher	Publication year
UOS, SINTEF, UOI	Workshop paper	ACM Digital Library as part of the ACM ICPS program (TBA)	A Way Forward for the MDCG 2019-16 Medical Device Security Guidance	Steve Taylor	PErvasive Technologies Related to Assistive Environments (PETRA) 2024	ACM	2024
SINTEF, UOS	Conference paper	ISSN 1613-0073, Vol-3674 https://ceur-ws.org/Vol-3674/RP-paper6.pdf	Dynamic Cyber Risk Assessment for Connected Medical Devices: the NEMECYS Approach	Gencer Erdogan	18th International Conference on Research Challenges in Information Science	Springer	2024

6.1.2 Participation in events

Partner(s)	Type of activity	Place & Date of Activity	Description of the activity	Title of activity/event	Type of Audience	Size of Audience	Countries addressed	Link
SINTEF	Poster	Lisbon, Portugal, 22-24 February 2023	Present the objectives and main goals of the NEMECYS project.	International Conference on Information Systems Security and Privacy (ICISSP 2023)	Research communities	ca. 100 people	International	https://www.insticc.org/node/TechnicalProgram/ICISSP/2023/presentationDetails/641

Partner(s)	Type of activity	Place & Date of Activity	Description of the activity	Title of activity/event	Type of Audience	Size of Audience	Countries addressed	Link
UOS, ATC, SINTEF	Meeting, discussion	Munich, Germany, 24-25 May 2023	NEMECYS Representa-tion at NESSI thought leadership meeting 24-25 May 2023	NESSI Meeting	Research communities	about 30 people	Europe	N/A
SINTEF	Presentation	Trondheim, Norway, 3 April 2024	Presentation at DND/ISF/-ISACA/CSA meetup	Meeting	IT professionals	about 20 people	Norway	N/A
SINTEF, UOS	Poster, Roll-up	Guimarães, Portugal, 14-17 May 2024	NEMECYS Project presentation	18th International Conference on Research Challenges in Information Science	Research communities	about 80-100 people	International	https://www.rcis-conf.com/rcis2024/
SINTEF	Presentation	Oslo, Norway, 11 January 2023	Presentation of the NEMECYS project	"HealthWorld" workshop	Stakeholders (Industry, business partners)	73	Norway	N/A
SINTEF	Networking	Oslo, Norway, 31 January 2023	Participation in the networking event	"Secure digital transformation in healtcare", arranged by Norway Health Tech in Oslo, Norway	Stakeholders (Industry, business partners)	150	Norway	https://www.norwayhealthtech.com/event/sikre-smarte-sykehus/

Partner(s)	Type of activity	Place & Date of Activity	Description of the activity	Title of activity/event	Type of Audience	Size of Audience	Countries addressed	Link
SINTEF, ATC	Presentation	Online networking event, 8 March 2023	Presentation of the NEMECYS project	Introductory online meeting (1 hour) for the sibling projects (funded by HaDEA), arranged by NEMECYS	Research communities	9	Europe	N/A
SINTEF, ATC	Presentation	Online networking event, 23 March 2023	Presentation of the NEMECYS project	Networking meeting for the new Horizon Europe Health projects, arranged by HaDEA	Research communities	About 10 people	Europe	N/A
OSR	Presentation	Online meeting, 10 January 2023	Presentation of the NEMECYS project	Meeting with Cybersecurity department of Grupo San Donato	Cybersecurity professionals	4	Italy	N/A
SINTEF	Presentation	Trondheim, Norway, 28 April 2023	Presentation of the NEMECYS project	Norwegian Directorate of e-health divisional gathering on cybersecurity	Local authorities	25	Norway	N/A

Partner(s)	Type of activity	Place & Date of Activity	Description of the activity	Title of activity/event	Type of Audience	Size of Audience	Countries addressed	Link
SINTEF	Presentation	Online event, 3 June 2023	Presentation of needs and challenges for security in CMDs, and how we plan to address them in NEMECYS: "Connected Medical Devices Need Cybersecurity by Design Too"	IEEE CS DVP EXA Event	Research communities	Unknown	International	N/A
SINTEF	Presentation	Stakeholders' event, Lillehammer, Norway, 28 August 2023	Presentation of NEMECYS and good and bad aspects of the MDCG 2019-16 guidance for addressing the MDR.	Sikkerhetsfestivalen 2023	Stakeholders (Healthcare providers/operators)	20	Norway	https://sikkerhetsfestivalen-2023.sessionize.com/session/463788

Partner(s)	Type of activity	Place & Date of Activity	Description of the activity	Title of activity/event	Type of Audience	Size of Audience	Countries addressed	Link
SINTEF	Presentation	Meeting, Dubrovnik, Croatia, 17 October 2023	Presentation of NEMECYS for the Europaen Health Information and Analysis Centre (EH-ISAC)	EH-ISAC meeting	Stakeholders (Healthcare providers/operators)	20	International	https://h-isac.org/summits/2023-european-summit/
SINTEF	Presentation	Conference, Gardermoen, Norway, 22 November 2023	Presentation of stakeholder challenges from D3.1	Norm-konferansen	MD Manufacturers	21	Norway	https://www.ehelse.no/normen/normkonferansen-2023
SINTEF	Presentation	Hybrid event, Naples, Italy, 31 October 2023	Presentation of NEMECYS, and collaboration with the sibling projects	AI4HealthSec final event, Naples, Italy (online)	Research communities	20	International	https://www.ai4healthsec.eu/final-event/

Partner(s)	Type of activity	Place & Date of Activity	Description of the activity	Title of activity/event	Type of Audience	Size of Audience	Countries addressed	Link
IBM	Workshop Keynote	Hybrid event, Reykjavik University, Iceland, 25/6/2024	Presentation of the Privacy Challenges in the AI Era	ESPRE 2024 The 11th International Workshop on Evolving Security & Privacy Requirements Engineering	Research communities	15	International	https://cybersecurity.bournemouth.ac.uk/espre2024/
SINTEF	Presentation	Networking event, Trondheim, Norway, 31/01/2024	NEMECYS tools presentation	Meetup Dataforeningen, VitalThings,	Stakeholders (Industry, business partners)	15	Norway	N/A
SINTEF	Presentation	Open Public seminar, Forsknings-parken, Gaustadalleen 21, Oslo, Norway	Presentation of NEMECYS and how AI is applied in the project (WP2).	Public seminar: "Generative AI: Development and societal impact."	Society	101	Norway	https://www.sintef.no/arrangementer-og-kurs/arkiv/2024/generativ-ai-utvikling-og-samfunnspavirkning/

6.1.3 Events organised by NEMECYS

Partner(s)	Type of activity	Place & Date of Activity	Description of the activity	Title of activity/event	Type of Audience	Size of Audience	Countries addressed	Link
SINTEF and NEMECYS project partners	Workshop	Hybrid event Brussels, Belgium 06/07/2023	Collaboration with sibling projects for the elaboration of the MDCG guidelines and other topics of cooperation.	MDCG workshop	EU projects' partners	14 (+online participants)	Europe	
SINTEF	Workshop	Trondheim, Norway, 02/02/2024	Evaluation of the implementation of regulations, standards and best practices for connected medical devices	Workshop on Cybersecurity in the health sector	Manufacturers, Integrators, Operators	17	Norway	
RSH	Workshop	Online 21/03/2024 22/03/2024 25/03/2024	Evaluation of the implementation of regulations, standards and best practices for connected medical devices	Workshop (3 sessions) on Cybersecurity in the health sector	Manufacturers, Integrators, Operators	8	Spain	
OSR	Workshop	Online 11/04/2024, 22/04/2024	Evaluation of the implementation of regulations, standards and best practices for connected medical devices	Workshop (2 sessions) on Cybersecurity in the health sector	Integrators, care service providers, Operators	7	Italy	

Partner(s)	Type of activity	Place & Date of Activity	Description of the activity	Title of activity/event	Type of Audience	Size of Audience	Countries addressed	Link
UOI, ATC, PDN	Workshop	Online 12/04/2024	Evaluation of the implementation of regulations, standards and best practices for connected medical devices	Workshop on Cybersecurity in the health sector	manufacturers, integrators, care service providers, regulatory experts, and cybersecurity professionals	11	Greece, Europe	

6.1.4 Workshops

In the period of February to April 2024, the NEMECYS project organized a series of workshops (4) across Norway, Spain, Italy, and Greece as part of Task 1.2: "Adherence to guidelines and gaps for current and future uses". The workshop participants were medical device manufacturers, vendors, integrators, health operators, and cybersecurity experts.

The workshops aimed to assess how regulations, standards, and best practices are used by MD stakeholders (manufacturers, integrators, and care service providers). They investigated tensions between cybersecurity, ethics, and clinical care regulations, proposed resolution strategies, systematically reviewed current standards, guidelines, and best practices, identified gaps and requirements for current and future needs, analysed architectural requirements to identify vulnerabilities and recommendations.

In **Norway**, participants were recruited by **SINTEF** from local health technology ecosystem players, targeting individuals knowledgeable in regulations, standards, and cybersecurity guidelines. Out of 19 registrations, **17 participants** attended the physical workshop **(Trondheim, Norway, 02/02/2024).**

In **Spain, Ribera Salud** organized the workshop. The invitation format and participant list were decided, and a CDA was validated and sent to participants. Different contact methods were used for different stakeholders. There were 21 registrations, with **8 participants** attending three sessions focusing on manufacturers, integrators, and operators respectively. **(Online sessions, 21/03/2024, 22/03/2024, 25/03/2024)**

In **Italy, OSR** invited 22 people via direct email, shared a post on social media accounts, and distributed further invitations through different networks and intermediaries. Out of 10 registrations, **7 participants** attended two online sessions organized to accommodate conflicting schedules. **(Online sessions, 11/04/2024, 22/04/2024)**

In **Greece, UOI, PDN, and ATC** identified key stakeholders, including manufacturers, integrators, care service providers, regulatory experts, and cybersecurity professionals. They reached out through targeted emails, industry networks, and professional associations. There were 23 registrations, with **11 participants** attending the online workshop. **(Online workshop, 12/04/2024)**

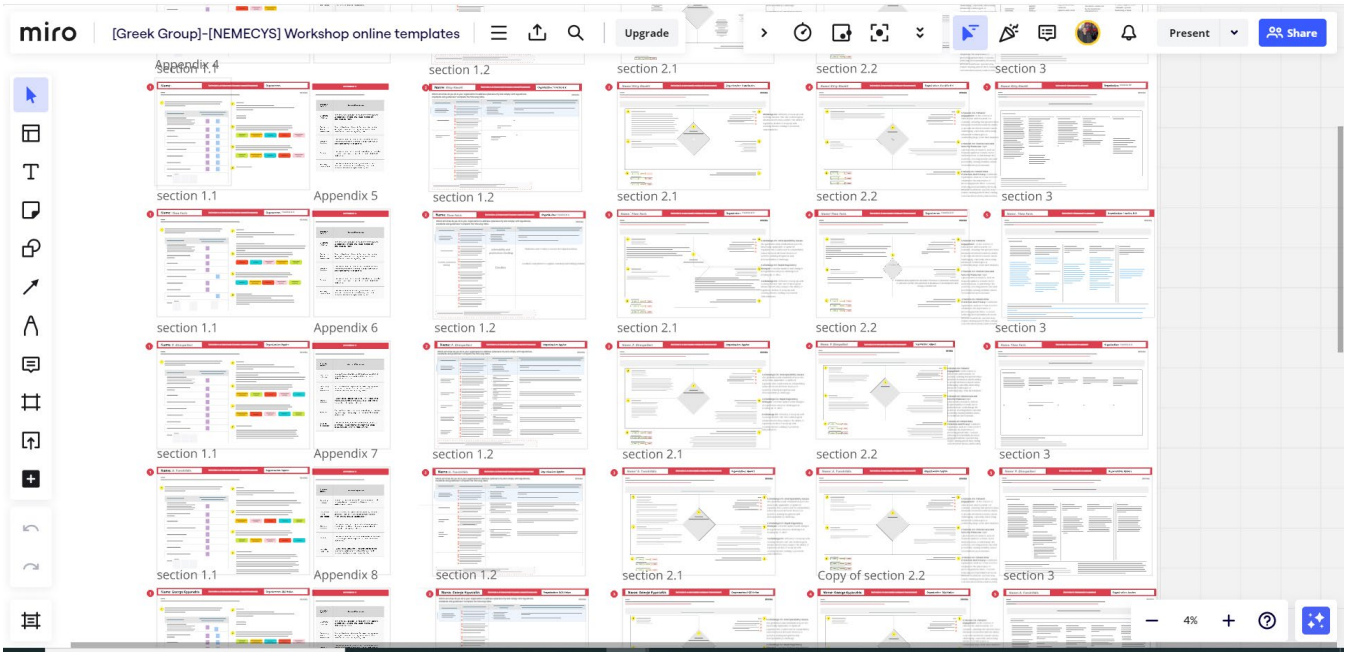


Figure 16: NEMECYS virtual workshop (MIRO board).

Overall, these workshops facilitated a comprehensive evaluation of the current implementation of regulations, standards, and best practices, identified significant gaps and requirements for future needs, and contributed valuable insights to enhance the cybersecurity and regulatory framework for connected medical devices, as detailed in D1.2 Systematic Review of Documentation (Final).

6.1.5 Collaboration activities with sibling projects

The sibling projects NEMECYS, SEPTON, ENTRUST, MEDSECURANCE and CYLCOMED under the HORIZON-HLTH-2022-IND-13-01 umbrella have established a robust collaboration framework aimed at enhancing cybersecurity for medical devices (Annex 10.2). Key areas of collaboration include:

- Refining the MDCG guidelines: The projects are actively involved in providing feedback and suggesting improvements to the MDCG guidelines. We have initiated a joint effort to create a collaborative whitepaper addressing regulatory complexities and proposing enhancements.
- Developing security tools: Each project is developing specialized tools and toolkits to bolster security assurance for connected medical devices. MEDSECURANCE's "security assurance toolkit" is highlighted, with potential integration of tools from other projects to support a unified certification process.
- Coordinating dissemination efforts: Efforts are underway to synchronize dissemination and communication plans across the projects. This includes exchanging plans for stakeholder events and exploring opportunities for joint outreach to amplify project impacts.
- Addressing regulatory challenges: Discussions focus on navigating regulatory landscapes, particularly regarding the Medical Device Regulation (MDR) and relevant standards (e.g., ETSI EN

303 645). The projects are pooling resources to influence guidelines and ensure alignment with evolving cybersecurity requirements.
- Exploring future collaborations: Beyond immediate objectives, the projects are identifying new areas for collaboration such as risk assessment methodologies, standards development, and case study exchanges. Future joint activities and scientific publications are also being considered to leverage collective expertise.

In the initial stages of the NEMECYS project, the coordination team actively sought collaboration with SEPTON, ENTRUST, MEDSECURANCE, and CYLCOMED, starting from the third month at the project officer's encouragement.

The first joint (online) meeting organized by NEMECYS on March 8, 2023, included active participation from SEPTON, ENTRUST, and MEDSECURANCE, marking a pivotal moment for future cooperation. Immediate actions included sharing presentation slides among SEPTON, ENTRUST, and MEDSECURANCE to ensure mutual access to progress and insights. NEMECYS also arranged a dedicated session to discuss early findings on the MDCG guidelines, facilitating detailed exchanges of ideas and methodologies.

NEMECYS led efforts to synchronize dissemination and communication plans across sibling projects offline, identifying opportunities for cooperation and streamlining strategies to enhance collective impact. ENTRUST proposed organizing a joint workshop for all five projects by late 2023, initiating positive discussions in the spring. These early interactions established a collaborative foundation for ongoing engagement.

Following these efforts, NEMECYS continued to build momentum by participating in a **networking session hosted (online) by HaDEA on March 23rd, 2023**. The session began with introductions from the HaDEA team, outlining their role and discussing EU grant management, though less relevant to NEMECYS' medical research focus.

During the breakout session for IND-13-01, NEMECYS reconnected with SEPTON, ENTRUST, and MEDSECURANCE, exploring potential collaborative activities. Discussions included plans by ENTRUST and MEDSECURANCE to deliver reports on MDCG guideline enhancements, with ENTRUST aiming for December 2023 and MEDSECURANCE planning to verify recommendations through use cases similar to NEMECYS' approach. SEPTON expressed interest despite their primary focus on privacy and GDPR rather than MDCG. ENTRUST also announced intentions to release a white or policy paper by fall 2023, inviting contributions from other projects. All parties indicated interest in participating in a joint MDCG workshop tentatively scheduled for June/July.

Regarding connected medical device requirements and security tools, SEPTON and NEMECYS aligned deliverables, focusing on specifications, while MEDSECURANCE's "security assurance toolkit" offered opportunities for collaboration, particularly in certification processes.

Discussions on dissemination and communication events included plans for shared stakeholder events, supported by HaDEA's commitment to promoting and amplifying results. Post-meeting discussions led to plans for a Brussels workshop in July 2023, aimed at strengthening collaborative efforts and sustaining momentum.

The **MDCG workshop concertation (hybrid) event, held on July 6th, 2023, at SwissCore - Norcore premises in Brussels**, organised by NEMECYS, aimed to achieve several key objectives. Participants (14, plus online participants) from NEMECYS, MEDSECURANCE, ENTRUST, SEPTON, and CYLCOMED attended, focusing on sharing initial experiences with the MDCG 2019-16 guideline, identifying challenges, and proposing enhancements. Presentations from each project highlighted regulatory complexities and outlined feedback on the guidelines. Discussions resulted in plans to collaboratively draft a whitepaper offering feedback and recommendations, with leaders appointed to oversee this effort and engage with the Project Officer for timeline alignment. Areas for future collaboration, including risk assessment, standards development, case studies, and stakeholder events, were identified. Participants expressed enthusiasm for continued collaboration through regular calls and meetings, with action points set for documenting minutes, establishing a shared workspace, and progressing the MDCG whitepaper and risk assessment initiatives.

Follow-up (online) **meetings** in **September 2023, October 2023 and January 2024** refined the collaborative initiatives, including developing the MDCG whitepaper and preparing scientific publications and conferences. By January 24th, 2024, discussions continued on advancing the whitepaper and exploring additional collaboration, demonstrating ongoing commitment to enhancing cybersecurity frameworks for connected medical devices through shared knowledge and aligned methodologies.

On **June 28th, 2024, a second face-to-face meeting** was arranged, in conjunction with the PErvasive Technologies Related to Assistive Environments (PETRA) conference in Crete. Participants from NEMECYS, SEPTON and CYCLOMED attended this meeting, where a refinement of the joint project feedback on the MDCG guidelines and further collaboration activities were discussed.

6.1.6 Clustering activities

NEMECYS, a project dedicated to enhancing the cybersecurity of connected medical and diagnostic devices (CMDs), **joined the ECSCI cluster[5] on February 23, 2024**. The European Cluster for Securing Critical Infrastructures (ECSCI), comprising 35 EU-funded projects, aims to bolster critical infrastructure protection and resilience through collaborative innovation and cross-project synergies. This alignment offers a strategic advantage for NEMECYS as it addresses the urgent need for robust cybersecurity in the rapidly evolving European healthcare landscape, which increasingly relies on personalized, distributed, and home-based services facilitated by CMDs.

[5] https://www.finsec-project.eu/ecsci

Figure 17: The ECSCI cluster.

As CMDs become integral to healthcare, they face significant cyber threats that could jeopardize patient safety and well-being. The NEMECYS project is crucial in developing tools and procedures to ensure cybersecurity by design for these devices. By joining the ECSCI cluster, NEMECYS seeks to leverage collaborative efforts to enhance its research and development activities, drawing on the collective expertise and innovations of the cluster.

In summary, joining the ECSCI cluster allows NEMECYS to harness the power of collective innovation and expertise. This strategic move will enable NEMECYS to contribute to and benefit from the broader efforts to protect critical infrastructures, fostering a safer and more resilient healthcare ecosystem.

6.1.7 External Advisory Board (EAB) formation and initial meeting

The NEMECYS project is set to benefit from the guidance of its newly formed External Advisory Board (EAB), a group composed of recognized, independent experts in cybersecurity risk management, connected medical devices, and other advanced technologies relevant to the project's research. These

experts have been invited to assist in the decision-making process, especially in situations that require specific technical expertise.

The organization of the EAB followed a meticulous process. Initially, project partners were invited to review their professional contacts for potential candidates. A comprehensive list of these candidates was then created, and each individual's profile and expertise were carefully evaluated. From this pool, a select group of highly qualified experts in the necessary domains was chosen. The project team reached out to these experts through the partners to confirm their availability. Upon receiving positive responses, official invitations were sent out to the selected candidates, inviting them to become members of the EAB. With the board members confirmed, **the first meeting of the EAB was organized on December 13, 2023**.

The meeting opened with introductions from EAB members, representing the following organizations:

- **Norwegian Directorate for eHealth,**
- **Tampere University,**
- **BD (Becton, Dickinson and Company), and**
- **PKNM Solutions Sárl.**

An overview of the NEMECYS project was presented, followed by a discussion on the suitability of ISO 14971 for risk-benefit assessment and patient safety, noting its limitations in technical cyber risk management. The 2019 version of ISO 14971 was highlighted as an improvement and widely adopted in the EU, US, and China. Discussions centered on efforts to provide feedback on the MDCG-2019-16 guideline through a white paper, though direct connections with its authors have not yet been established. The forthcoming Cyber Resilience Act (CRA) will set higher cybersecurity standards for digital products, prompting enhancements aligned with MDCG requirements, especially for healthcare providers managing high cyber risk equipment.

The EAB suggested reevaluating the focus on device approval processes and recommended engaging Notified Bodies and Competent Authorities more actively. They welcomed insights and references to similar initiatives for documentation, standards, guidelines, and tools. BD contributed insights on SBOM (Software Bill of Materials) and Legacy Devices, involved in MedTech Europe and the ENISA cybersecurity certification group. Useful documentation will be thoroughly reviewed, and the meeting slides are available for distribution.

The meeting concluded with a consensus on strengthening the technical aspects of cyber risk management within the NEMECYS project. Future steps include:

- Initiating enhanced collaboration with Notified Bodies and Competent Authorities to refine device approval processes.
- Integrating valuable insights and documentation from EAB members.
- Continuing to explore and leverage external resources and guidelines to bolster cybersecurity measures across connected medical devices and related technologies.

These efforts aim to fortify the project's framework and ensure robust cybersecurity practices to safeguard against emerging threats in healthcare technology.

6.1.8 Press releases and web presence

Type	Webpage
Short Description	Since the beginning of the project, a brief summary of the NEMECYS was presented on the SINTEF website (Norwegian, English).
URL	https://www.sintef.no/en/projects/2023/nemecys-new-medical-cybersecurity-assessment-and-design-solutions/ https://www.sintef.no/prosjekter/2023/nemecys-nye-risikovurderingsmetoder-og-designlosninger-for-cybersikkerhet-i-medisinteknisk-utstyr/

Type	Webpage
Short Description	Since the beginning of the project, a brief summary of the NEMECYS was presented on the ATC company's website.
URL	https://ilab.atc.gr/portfolio/nemecys/

Type	Magazine article
Short Description	An article presenting the NEMECYS project was published on the Norwegian MEDWATCH magazine website on January 12, 2023.
URL	https://medwatch.no/nyheter/medtek_lab/article14827919.ece

7 Dissemination & communication impact assessment

During the initial 18-month period, NEMECYS achieved significant milestones in its dissemination and communication efforts. This included the **publication of 5 refereed scientific articles** (a further 3 have been accepted for publication), progressing towards the project's goal of 20 publications by its conclusion.

The project successfully **organized 4 workshops held in Spain, Italy, Greece, and Norway**, with the participation of 43 stakeholders' representatives. The aim was to conduct 3 thematic workshops by the project's end.

Additionally, a **workshop convened in Brussels with 14 participants from NEMECYS** sibling projects facilitated collaborative discussions. In addition to that the project regularly organise and participates in online meetings with sibling projects (4 meetings).

NEMECYS actively **participated in 5 scientific conferences** during this period, with a target of 7 by project completion. The project also engaged in over 23 events, approaching target of 24 by the project's end, encompassing conferences, workshops, and stakeholder meetings.

NEMECYS further enhanced its network by **joining the European Cluster for Securing Critical Infrastructures (ECSCI)**, which includes 35 EU-funded projects, fostering broader collaboration within the cybersecurity domain.

Online visibility efforts included the **NEMECYS website attracting 524 visitors**, **LinkedIn establishing 83 followers with 34 posts**, and **Twitter reaching 48 followers, achieving 941 impressions through 52 posts**, thereby expanding its outreach in the cybersecurity and medical device sectors.

8 Future plans

The project will focus on updating its website content to present the latest NEMECYS tools and scientific publications. Public awareness about the launch of the NEMECYS pilot will be created through the project's social media channels and website blog. Events such as workshops will be organized with stakeholders to demonstrate NEMECYS tools, showcase their features, and promote them effectively.

The collaboration with sibling projects will continue, particularly in the domains of MDCG guidelines and cybersecurity standards. The project use cases will be demonstrated, and interested parties from sibling projects will be invited for active participation.

The cooperation with the External Advisory Board will be enhanced to discuss pilot outcomes and their promotion. NEMECYS will actively engage with ESCSI cluster activities, participating in and co-organizing workshops and other events, promoting project results through the cluster.

Taking into account that the preliminary versions of the project technical and research outcomes will be introduced on month 18, it is important to seek opportunities to promote them in the organizations, associations, and regulatory bodies as defined in the deliverable D5.1 Dissemination and Communication Plan (Annex 10.1).

Close to the end of the project, a conference will be organised to demonstrate and promote the NEMECYS outcomes to stakeholders, including manufacturers, integrators, healthcare providers, cybersecurity experts, researchers, and policymakers. Consideration will be given to organising this conference in collaboration with the NEMECYS sibling projects.

The project will maintain active participation in various international conferences and events to disseminate findings and build networks within the cybersecurity and healthcare sectors.

8.1 Indicative dissemination events

- International Conference on Health and Social Care Information Systems and Technologies (HCist): Scheduled for November 13-15, 2024, in Funchal, Madeira, Portugal. https://hcist.scika.org/

- IEEE Secure Development Conference: Scheduled for October 7-10, 2024, at Carnegie Mellon University, Pittsburgh, PA. https://secdev.ieee.org/2024/home

- SecAssure@ESORICS: The 3rd International Workshop on System Security Assurance (SecAssure) will take place in Bydgoszcz, Poland, co-located with ESORICS 2024 from September 16-20. https://www.ntnu.edu/secassure

- Nordsec: The 29th Nordic Conference on Secure IT Systems will take place at Karlstad University from November 6-7, 2024. http://www.nordsec.org/conferences/

2025 Events:

- IEEE Symposium on Security and Privacy: Scheduled for May 12-14, 2025, with workshops on May 15, 2025, in San Francisco, CA. https://www.ieee-security.org/TC/SP2025/

8.2 Indicative scientific journals and specialized magazines

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
Health Informatics Journal	Sage Journals	https://journals.sagepub.com/home/jhi
Journal of Healthcare Informatics Research	Springer	https://link.springer.com/journal/41666

IBM already submitted the paper which is pending for approval. "Is My Data in Your Retrieval Database? Membership Inference Attacks Against Retrieval Augmented Generation" https://arxiv.org/abs/2405.20446v2 to DPM 2024 the 19th DPM International Workshop on Data Privacy Management.

9 Conclusions

Based on the extensive dissemination, collaboration, and clustering activities detailed in the NEMECYS project has made great strides toward accomplishing its dissemination and communication goals:

- NEMECYS has effectively disseminated its findings through a variety of channels, including scientific publications, conference papers, workshops, and participation in international events. These efforts have not only shared critical insights on cybersecurity for connected medical devices (CMDs) but also positioned the project prominently within global research communities.
- The collaboration with sibling projects under the HORIZON-HLTH-2022-IND-13-01 umbrella has been pivotal. NEMECYS actively contributes to refining MDCG guidelines, coordinating dissemination efforts, and addressing regulatory challenges. This collective approach enhances the impact of each project and accelerates advancements in CMD cybersecurity.
- Through 4 targeted workshops across multiple European countries, NEMECYS has engaged stakeholders comprehensively, assessing current regulatory adherence and identifying future cybersecurity needs for CMDs. Joining the ECSCI cluster further strengthens NEMECYS' position by leveraging collaborative innovation to enhance CMD cybersecurity within critical infrastructures.
- The formation of an External Advisory Board comprising cybersecurity and medical device experts underscores NEMECYS' commitment to robust governance and technical excellence. Insights from the EAB have guided strategic decisions and enhanced the project's alignment with international standards and regulatory frameworks.

In conclusion, NEMECYS has not only made significant strides in advancing CMD cybersecurity but has also fostered a collaborative ecosystem that amplifies its impact. By disseminating knowledge, engaging stakeholders, leveraging cluster synergies, and benefiting from expert guidance, NEMECYS is poised to contribute substantially to securing connected medical devices in healthcare settings globally.

10 Annexes

10.1 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/)	RSH	Active membership participation.
Healthcare Information and Management Systems Society (https://www.himss.org/)	RSH	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	UoS	Partner

sits at the centre of the £33M Trustworthy Autonomous Systems Programme, funded by the UKRI Strategic Priorities Fund.		
NHS England - Transformation Directorate https://transform.england.nhs.uk/ supports transformation to improve health and care for everyone.	UoS	Contact

10.2 Annex: Sibling projects

Name	Description	Contact / URL
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)	https://www.medsecurance.org/
SEPTON	"Sibling" project funded under the HORIZON-HLTH-2022-IND-13-01 topic. Coordinated by SPACE HELLAS SA (EL)	https://septon-project.eu/