HORIZON-HLTH-2022-IND-13-01

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

NEMECYS
New Medical Cybersecurity and design Solutions

D5.2 Exploitation Plan (Initial)

Project Reference No	NEMECYS – 101094323
Deliverable	D5.2 Exploitation Plan (Initial)
Work package	WP5: Dissemination, Exploitation and Outreach
Type	R - Document, report
Dissemination Level	PU - Public (fully open)
Date	30/06/2023
Status	Final
Editor	Colin Upstill (ICE)
Contributors	Karin Bernsmed, Gencer Erdogan, Lars Flå and Nektaria Kaloudi (SINTEF); Gøran van den Burgt (MODE); Maya Anderson (IBM); George Zissis (ATC); Salvador García (MS); Mariet Nouri (OSR); Christos Androutsos (UoI); Steve Taylor (UoS); Colin Upstill (ICE); George Rigas (PDN); Stefan Proennecke (DB)
Reviewers	Margarita Koromila (ATC); Vasilis Pezoulas (UoI)
Document description	Preliminary analysis identifying exploitable items and first draft exploitation plans for each, taking communication activities into account.

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	18/05/2023	Draft 1	Colin Upstill
v0.2	08/06/2023	Draft 2	All Contributors
v0.3	29/06/2023	Review	Margarita Koromila, Vasilis Pezoulas and Colin Upstill
v1.0	30/06/2023	Final version	Karin Bernsmed

Executive Summary

NEMECYS exploitation will be wide-ranging and high impact regarding the enhanced cybersecurity of Connected Medical Devices (CMDs), and potentially in many other sectors and applications where Internet of Things (IoT) devices share confidential or sensitive data.

This deliverable presents the initial exploitation plan for NEMECYS, setting out the exploitation strategies for commercialisation, open source (community exploitation and commercial services), consultancy services, further research, policy making, and education and training. Exploitation policies, pathways and tools established for Horizon Europe are reviewed and potential benefits for NEMECYS noted. Expected exploitable results are summarised, and initial exploitation plans for each are set out.

Table of Contents

List of Tables

List of Abbreviations

Abbreviation	Definition
CMD	Connected Medical Device
CORDIS	Community Research and Development Information Service
cPPPs	contractual Public-Private Partnerships
EC	European Commission
EIC	European Innovation Council
ERC-POC	European Research Council Proof of Concept
ERA	European Research Area
EU	European Union
HaDEA	European Health and Digital Executive Agency
HRB	Horizon Results Booster
HRP	Horizon Results Platform
HSBooster	Horizon Standardisation Booster
ICT	Information and Communications Technology
IoT	Internet of Things
IP	Intellectual Property
IPR	Intellectual Property Rights
MD	Medical Device
PESTLE	Political, Economic, Social, Technological, Legal and Environmental
R&D	Research and Development
R&I	Research and Innovation
SaaS	Software as a Service
SAM	Scientific Advice Mechanism
SaMD	Software as Medical Device
SERI	State Secretariat for Education, Research and Innovation
SSM	System Security Modeller
SWOT	Strengths, Weaknesses, Opportunities and Threats
TRL	Technology Readiness Level
UKRI	UK Research and Innovation

1 Introduction

Exploitation is about making concrete use of results for the benefit of innovation, the economy and society. Exploitation planning for NEMECYS results involves the identification of exploitable items and a suitable impact plan for each, considering aspects such as the most appropriate exploitation strategy (e.g. commercial exploitation, open source, further research), the aspirations of the exploiting partners, the needs of the target user base, the potential market, time to market, end-users, benefits, TRL (Technology Readiness Level [1]), competing technologies, further R&D needed, further investment needed, appropriate means for the protection of foreground IP, partners/third parties interested, etc.

1.1 Purpose and scope

This initial Exploitation Plan identifies potential exploitable items and first draft exploitation plans for all partners. Possible exploitation channels are discussed. Initial investigations during the first six months of the project are reported. The exploitable results and exploitation plans may change during the implementation of the project.

1.2 Methodology and structure of the deliverable

This deliverable has been created based on the experience of the project's Exploitation Manager and those in the project's Exploitation Committee.

The deliverable is structured as follows:

- Section 2 introduces our exploitation strategy.
- Section 3 outlines the expected exploitable results from the project.
- Section 4 explains our exploitations plans.
- Section 5 concludes the report.

2 Exploitation strategy

NEMECYS exploitation will be wide-ranging and high impact regarding the enhanced cybersecurity of connected medical devices (CMDs), and potentially in many other sectors and applications where IoT devices share confidential or sensitive data.

NEMECYS has established IPR management appropriate to ensure this, including an IP Register which will be maintained throughout the project. The general principles for handling Knowledge and IPR are defined in the Grant Agreement and in the Consortium Agreement, in line with Horizon Europe IPR recommendations.

NEMECYS exploitation will include commercial exploitation of products and services; community exploitation of open-source software using various channels; cybersecurity awareness consultancy services and further research to address future technological and other developments.

The exploitation strategy begins with the determination of a list of exploitable results and potential user segments, based on the NEMECYS tools and target groups set out above, followed by determination of the most appropriate exploitation plan per result, considering the exploiting partners and the target community, which will then be consolidated into an overall exploitation plan, resolving any conflicts or inconsistencies and ensuring that they all contribute to the overall objective of sustainably maximising benefit for all stakeholders.

NEMECYS exploitation will take into account the communication activities set out in the deliverable D5.1 "Dissemination and Communication plan", which provides a comprehensive framework for actions that will support outreach to stakeholders.

The exploitation actions will conclude with the preparation of materials for information campaigns, introducing the main innovations (using slides, posters, and a video), and giving more detailed information (e.g., via white papers). These materials will be appropriate for use online and to promote the NEMECYS results at physical events and meetings, via channels identified by project partners and in collaboration e.g., with the Horizon Results Platform [11].

The effectiveness of the exploitation strategy will be measured using the success metrics set out in the project's pathways towards impact, viz.

- Outcome 1: Stakeholders (e.g., manufacturers, suppliers, health care providers, integrators, operators) apply measures to identify and address cybersecurity risks and gaps in connected medical devices.
- Outcome 2: Stakeholders adopt and use newly developed risk benefit analysis schemes and capabilities for cybersecurity of connected medical devices.
- Outcome 3: Stakeholders adopt and use newly developed methodologies and toolboxes for ensuring cybersecurity of connected medical devices by design.
- Outcome 4: Stakeholders adopt and use fit for purpose guidance covering challenges posed by connected medical devices, including software.

2.1 Commercialisation

NEMECYS commercial exploitation will be driven by a Market Analysis, as a complete assessment of the size and nature of a market for a product or service. It will take into account both quantitative factors, such as the volume and value of the market, and qualitative factors, such as competition and regulation (see, e.g., NetMBA [2]). This will be followed by a PESTLE analysis [3], considering the barriers to success in relation to the expected impacts along Political, Economic, Social, Technological, Legal and Environmental axes, which in this context is about the result owner's organisation in the context of a market and is based on analysis of the trends that influence exploitation success. Finally, there will be a SWOT analysis considering the Strengths, Weaknesses, Opportunities and Threats in respect of the proposed exploitation. Based on the Market, PESTLE and SWOT analyses, which constitute a detailed review of the potential market opportunities, result owners will then identify potential business models and go on to undertake a financial assessment to determine which business models and customer segments to focus on.

2.2 Open-source strategy

Open-source strategies are an important part of the NEMECYS exploitation strategy. However, the strategy does not preclude other models of software licensing (e.g., SaaS, proprietary), especially if this helps exploitation.

The drivers of open source include: optimizing the cost of an ICT solution; fostering the extensive reusability of code; democratizing access to essential and basic software for everyone (by removing barriers to access technology and empowering people); speeding up ICT innovation (by allowing others to build up on prior work - similar to the process of science, where researchers base their work on earlier findings); sharing knowledge and practices to speed up software development; fostering interoperability by using standard and open technologies (when more and more software systems are built on many different technologies); community exploitation, where the results are made available as a public good; and building a successful business by offering services based on open source software, often including a freemium strategy in which software with enhanced functionality is made available under a paid-for licence.

It should be noted that using open source does not necessarily come without cost, it is not always free, and it does not always fit into all business models. The license terms must be followed, and it may not fit completely to all needs.

With open source, choices for support include building up know-how internally, contracting a third party, or relying on an active community. NEMECYS exploitation will utilise a variety of open-source licensing strategies, appropriate to the drivers that apply.

2.3 Consultancy services

Several NEMECYS partners envisage providing consulting, customer support and training services on a commercial basis. Possibilities include the following.

- Specific consultancy - identifying how customers will use a toolkit and doing the design work for them. This would include tailoring to the customers' needs and their specific business. Following the consultancy work, the customer would take over installing and using the toolkit.
- Installation and providing consultancy - tailoring the toolkit to the customers' needs and their specific business and installing it for them, and providing related consultancy services.
- Providing ongoing support - some customers may not have either the capability or the capacity to provide ongoing support for a toolkit installation.
- Toolbox-as-a-service – taking (parts of) the toolkit and using it on the customer's behalf, collecting input from the customer, and presenting the result afterwards.
- Training - providing customers with specific training to meet the needs of their business.

2.4 Further research

In addition to any commercial exploitation, including open source, partners will use the results to support further research, with the long-term benefit of contributing to the body of knowledge of cybersecurity, especially but not exclusively for CMDs.

2.5 Policy making

The NEMECYS project aims to contribute to policy making, primarily at the EU level, but also at local and regional levels in the countries where the project partners are established or do business. The project plans to produce policy guidelines and/or policy briefs (2-4 pages each), targeted at different levels of governance. The Medical Device Coordination Group [4], which is composed of representatives from all Member States, is one of several potential recipients.

2.6 Education and training

Some of the project partners, in particular the universities and research organisations, will use NEMECYS results in training events with selected stakeholders, and use them for other educational purposes in their own organisations and/or for their customers.

2.7 Exploitation in Horizon Europe

2.7.1 Policy: Valorisation in Horizon Europe

The EU Valorisation Policy [5], an integral part of Horizon Europe, aims to maximize the impact of research and innovation by translating knowledge into practical solutions with high socio-economic value. It plays a crucial role in Europe's transformation towards a greener, digital, inclusive, and sustainable society. The policy focuses on knowledge transfer and collaboration between industry and academia, identified as key milestones for the European Research Area (ERA) for Research and Innovation.

The European Council demonstrates a strong political commitment to support the EU valorisation policy and actively reviews and updates intellectual property management in knowledge transfer activities. The

policy review conducted by the European Commission identifies six main channels for knowledge valorisation: academia-industry collaboration, research-driven spin-offs and start-ups, intermediaries and knowledge transfer, citizen engagement, IP management and standardization, and knowledge dissemination and policy uptake.

To foster academia-industry collaboration, the EU supports initiatives such as contractual public-private partnerships (cPPPs), Future and Emerging Technology Flagships, and Marie Skłodowska-Curie Actions. These initiatives facilitate the exchange of academic knowledge with industry, enhancing researchers' skills and providing a better understanding of industry needs.

The EU has established programs like the European Innovation Council (EIC) and the European Research Council Proof of Concept (ERC-POC) to provide structured access to finance for research-driven spin-offs and start-ups. These programs enable students and academics to commercialize their developed knowledge and innovations.

Intermediary organizations, such as knowledge transfer offices, technology transfer offices, business incubators, and science parks, play a crucial role in helping researchers and innovators commercialize their solutions. They provide support, networking opportunities, mentoring activities, and best practices exchange to boost innovation potential.

Engaging citizens and public bodies is essential to ensure that new knowledge leads to innovative solutions that address societal needs. The EU encourages citizen involvement and recognizes their demand for science-based solutions. Initiatives like the European Capital of Innovation (iCapital) Award promote citizen engagement to accelerate the use of research results for the benefit of all.

Intellectual property management and standards are crucial factors in knowledge valorisation. A well-managed IP framework and adherence to standards contribute to innovation, creativity, knowledge sharing, and market accessibility. The EU provides support for IP management through services like the European IPR Helpdesk, Horizon IP Scan, and IP Booster. Standards also play a vital role by providing a common language for researchers, industry, and consumers, facilitating communication, interoperability, and consumer trust in innovative technology.

Knowledge dissemination and policy uptake are vital for data-informed policy making. The EU promotes open access to research results, data, models, and analyses to support decision-makers in understanding challenges and making informed decisions. Initiatives such as the Horizon Results Platform, JRC Policy Lab, and Scientific Advice Mechanism (SAM) facilitate knowledge sharing and policy alignment. By aligning with the EU Valorisation Policy and leveraging the available initiatives, the NEMECYS project can benefit from enhanced collaboration, funding opportunities, support for commercialization, IP management guidance, and access to research results dissemination platforms.

2.7.2 Monitoring: Key impact pathways

Horizon Europe legislation categorizes three types of contributions to societal impact: scientific, societal, and economic, which are tracked through nine Key Impact Pathways:

- Scientific impact: (1) Creating high-quality new knowledge; (2) Strengthening human capital in R&I; (3) Fostering diffusion of knowledge and Open Science;
- Societal Impact: (4) Addressing EU policy priorities & global challenges through R&I; (5) Delivering benefits and impact via R&I missions; (6) Strengthening the uptake of R&I in society; and
- Economic/Technological Impact: (7) Generating innovation-based growth; (8) Creating more and better jobs; and (9) Leveraging investments in R&I.

These pathways provide a framework for monitoring and assessing the impact of projects. The program emphasizes the dissemination and exploitation of results to maximize the impact of EU-supported R&I. It introduces measures such as proposal redesign, continuous reporting, and reinforced IP management to support effective knowledge transfer and utilization.

The implementation of Key Impact Pathways represents a modernized monitoring approach in Horizon Europe. This approach acknowledges the need to focus on achieving impact beyond research excellence. By incorporating consistent monitoring tools, the program aims to track impact on a granular level. Communication, dissemination, and exploitation of results are highlighted as essential means through which Horizon Europe projects can maximize their impact within this framework. By prioritizing impact, the EU aims to address the challenge of bridging the gap between research outcomes and their real-world application, leading to greater societal and economic benefits.

Overall, the valorisation policy and the novelties introduced in Horizon Europe emphasize the importance of effectively translating research results into tangible solutions with broader societal and economic implications. By providing guidance, tools, and monitoring mechanisms, the EU aims to enhance the impact of EU-supported R&I projects, promote knowledge dissemination, and foster collaboration and innovation across Europe.

NEMECYS can benefit from enhanced collaboration opportunities, funding support, knowledge transfer, and access to research results dissemination platforms, enabling the translation of their research into practical solutions with high socio-economic value.

2.7.3 European Commission tools

2.7.3.1 Research and innovation success stories

The European Commission (EC)'s Research and Innovation website [6] features success stories that highlight the achievements and impact of EU-supported research and innovation projects. These stories showcase scientific breakthroughs, technological innovations, and collaborations across various fields. They provide inspiring examples of project outcomes and their contributions to society, demonstrating the positive results and advancements resulting from European research and innovation efforts.

Publishing the results of the NEMECYS project as a success story on the EC's Research platform can greatly benefit the project's exploitation efforts. By sharing its outcomes, methodologies, and advancements in cybersecurity for connected medical devices, the project gains visibility among potential stakeholders, collaborators, and investors. This increased visibility can lead to

commercialization opportunities, industry partnerships, and further development of the project's results. The success story serves as a validation of the project's achievements, enhancing its reputation and credibility. It also facilitates knowledge exchange and learning, inspiring others in the field and contributing to the overall advancement of healthcare cybersecurity. Ultimately, publishing the project's results as a success story helps maximize the exploitation potential and impact of the NEMECYS project.

2.7.3.2 CORDIS

The Community Research and Development Information Service (CORDIS) [7] is the EC's primary source of results from the projects supported by the Framework Programmes.

CORDIS supports the exploitation of project outcomes by increasing their visibility, facilitating networking and collaboration, promoting knowledge dissemination, providing access to funding opportunities, offering policy guidance, and sharing best practices through success stories. Utilizing the resources and services available on CORDIS can enhance the chances of successful exploitation and maximize the impact of the project's outcomes.

By leveraging the resources and services available on CORDIS, the NEMECYS project can enhance the visibility of its outcomes, foster collaborations, disseminate its results, access funding opportunities, stay informed about relevant policies, and learn from successful projects. These elements collectively would contribute to the successful exploitation and impact of the NEMECYS project.

2.7.3.3 Horizon Dashboard

The Horizon Dashboard [8] presents success stories from EU supported projects, as well as data on participation in projects and on project performance. Projects can benefit from the Horizon Dashboard in multiple ways. Firstly, it promotes data transparency by allowing projects to share their progress, outcomes, and impact with the public. Secondly, the platform enables projects to explore and analyse their own data, identifying trends and insights for strategic decision-making. Additionally, projects can benchmark their performance against others, foster collaboration and networking opportunities, engage stakeholders, and utilize program data for evaluation and reporting purposes. Overall, the Horizon Dashboard enhances a project's visibility, performance, and impact within Horizon 2020 and the wider research and innovation community.

2.7.3.4 Horizon Results Booster

The Horizon Results Booster (HRB) [9] is an initiative that provides free consulting services to research projects supported by EU programs. HRB aims to maximize the societal impact and market potential of these projects by enhancing their exploitation strategies and value. The Horizon Results Booster offers three types of services:

- Portfolio dissemination & exploitation strategy:
    - Module A: Identifying and creating a portfolio of research and innovation project results.
    - Module B: Designing and executing a portfolio dissemination plan.
    - Module C: Improving existing exploitation strategies.
- Tailor-made support services to develop a business plan.
- Assistance, coaching, and mentoring for go-to-market activities.

These services aim to help projects optimize their dissemination and exploitation strategies, develop business plans, and receive guidance and support for successful market entry.

The HRB services could assist the NEMECYS project in optimizing its dissemination and exploitation strategies, developing strong business plans, and receiving valuable support for successfully commercializing its cybersecurity solutions.

However, the HRB service is currently only funded until June 2024, and most NEMECYS results will be delivered after this, so the HRB may be of limited use to NEMECYS.

2.7.3.5 Innovation Radar

The Innovation Radar [10] is an EC initiative that identifies and supports high-potential innovations emerging from EU-supported research and innovation projects. It aims to increase the visibility of these innovations and connect them with potential users, investors, and collaboration opportunities. The Innovation Radar provides an online platform for innovators to showcase their projects, technologies, and market ambitions. It also organizes events and initiatives to facilitate networking and matchmaking. Through these efforts, the Innovation Radar promotes the exploitation and commercialization of EU-supported innovations, contributing to economic growth and addressing societal challenges.

The NEMECYS project can benefit from the Innovation Radar in several ways. It can increase its visibility and exposure by being featured on the platform, attracting potential users, investors, and collaborators. The project can participate in networking events to establish partnerships and collaborations. The platform also provides an opportunity for market validation, allowing the project to gather feedback and refine its commercialization strategies. Access to resources and support services, such as guidance on intellectual property and regulatory compliance, can assist the project in its exploitation efforts. Being recognized and featured on the Innovation Radar platform can enhance the project's credibility and attract further support and funding. Overall, the Innovation Radar offers valuable opportunities for the NEMECYS project to enhance its market presence, engage with stakeholders, and achieve successful exploitation and societal impact.

2.7.3.6 Horizon Results Platform

To facilitate the uptake of research results by various stakeholders, the Horizon Results Platform (HRP) [11] serves as a central hub for sharing project results, including publications, reports, datasets, and software. The platform aims to increase the visibility and exploitation of project results by connecting projects with potential users, stakeholders, and industry partners. It provides a user-friendly interface for searching and exploring project results, enabling users to browse projects by topic, sector, or keyword. The platform facilitates knowledge transfer, collaboration, and commercialization opportunities by showcasing innovative solutions and allowing users to engage with project representatives. The platform now offers enhanced guidance and tools to beneficiaries. Additionally, the newly introduced Horizon Results TV provides expert advice on exploiting research results and shares inspirational stories of researchers who have successfully transitioned into entrepreneurs. These resources aim to support researchers in effectively valorising their work. Overall, the HRP plays a crucial role in disseminating project outcomes and maximizing their impact by providing a centralized platform for promoting and exploiting research and innovation results.

The HRP may provide NEMECYS with several benefits. By uploading its results, the project may gain increased visibility and exposure to a global audience, making it easier for potential users, stakeholders, and industry partners to discover and engage with its work. The platform also facilitates knowledge transfer, allowing the project to share its research findings and publications, benefitting other researchers and practitioners in the field. Additionally, the platform offers exploitation and commercialization opportunities by showcasing the project's innovative solutions and attracting the interest of potential users, investors, and industry partners. The platform's networking and collaboration features enable the project to connect with similar projects, fostering collaboration, knowledge exchange, and synergy in the field of cybersecurity for connected medical devices. Overall, the Horizon Results Platform will enhance the NEMECYS project's visibility, collaboration prospects, and opportunities for exploiting its outcomes.

2.7.3.7 IPR Helpdesk

The IPR Helpdesk [12] is a service provided by the EC to assist EU-supported projects and organizations in managing and protecting their IPR. It offers free and confidential advice on various aspects of IP, such as patents, copyrights, trademarks, and trade secrets. The Helpdesk provides information, training materials, and personalized support to project coordinators and participants, helping them understand the importance of IP in research and innovation activities. It also organizes workshops and events to promote awareness and offers an online helpline for submitting questions and receiving expert advice. Overall, the IPR Helpdesk empowers projects and organizations to effectively manage their IP assets, maximize the exploitation of their research results, and navigate the complexities of IP protection.

By leveraging the services of the IPR Helpdesk, the NEMECYS project can protect and manage its IP assets effectively, explore commercialization opportunities, and maximize the impact of its research outcomes in the cybersecurity field.

2.7.3.8 HSBooster

The Horizon Standardisation Booster (HSBooster, [13]) is a 24-month EC initiative to provide expert services to increase and valorise project results through the creation or revision of standards. By leveraging the expertise and support provided by HSBooster, projects can benefit from the standardization process, which can enhance the interoperability, compatibility, and market acceptance of their innovations. This initiative helps projects navigate the complex landscape of standardization, ensuring that their results align with industry requirements and can be effectively integrated into existing frameworks. Ultimately, HS Booster aims to maximize the impact and exploitation of project results by leveraging the power of standardization.

By engaging with HSBooster, the NEMECYS project could benefit from tailored support in navigating the standardization landscape, aligning its solutions with industry requirements, and maximizing the impact and exploitation of its research results.

However, HSBooster service is currently only funded until January 2024, and most NEMECYS results will be delivered after this, so the HSBooster may be of limited use to NEMECYS.

3 Expected exploitable results

The currently identified expected NEMECYS exploitable items, exploiting partners and stakeholder beneficiaries are listed in the table below. The details may change during the execution of the project.

Table 1: Exploitable items.

#	Item	Exploiting partners	Stakeholder beneficiaries
EI1	Best practice for cybersecurity of CMDs	MS, SINTEF, ICE, OSR, UoI, PDN, DB, MODE	Manufacturers, System Integrators, Scenario Operators, Advisory & User Groups, Regulators.
EI2	Proportionate risk benefit schemes balancing cybersecurity, ethics and clinical benefit – research and tooling	SINTEF, UOS, IBM, ATC	Manufacturers, System Integrators, Scenario Operators, Academia
EI3	Customized toolbox for MD manufacturers	SINTEF, ICE, MS, OSR, ATC, DB, MODE	Manufacturers
EI4	Customized toolbox for CMD system integrators	SINTEF, ICE, MS, OSR, ATC	System Integrators, e.g., Hospitals, Care Providers
EI5	Customized toolbox for CMD operators	SINTEF, ICE, MS, OSR, ATC	Scenario Operators, e.g., Hospitals, Local Authorities, Care Providers

Details on the best practice for cybersecurity for CMDs (EI1) and the tools included in the customized toolboxes (EI3, EI4 and EI5) can be found in the WP3 deliverables:

- D3.1 "Requirements for toolboxes".
- D3.2 and D3.3 "Toolboxes for healthcare stakeholders" (initial and final versions).
- D3.4 Documentation and training material.

Details on the proportionate risk benefit schemes (EI2) can be found in the WP2 deliverables:

- D2.1 and D2.3 "Risk Benefit Schemes" (initial and final versions).
- D2.2 and D2.4 "Risk Benefit Tooling" (initial and final versions).

4 Exploitation plans

4.1 Exploitable item 1 - Best practice for cybersecurity of CMDs

The best practices from NEMECYS will be particularly sought after by start-ups and SMEs, as they may have less resources to devote to security. Given that these best practices will likely contain information applicable to several domains using embedded and connected systems, we foresee ripple effects outside of the medical domain. The best practices will be promoted in public deliverables on the project's website and shared on relevant online forums and social media.

Marina Salud (MS) is a paperless and fully digitalized hospital in which integration of data, applications and devices has been a core feature from the outset. This implies a high dependence on IT systems and makes cybersecurity a main concern for the organization. Therefore, MS is continuously seeking to improve its overall cybersecurity and will utilize the results obtained in NEMECYS to better assess the risks related with the connected medical devices and apply the best practices that minimize those risks. Moreover, MS will foster the utilization of the tools through dissemination activities in the public health network it is part of.

SINTEF will utilize the findings of the NEMECYS project to promote the adoption and application of best practices for cybersecurity of CMDs. The key stakeholders who will benefit include not only medical device manufacturers, system integrators, and operators such as healthcare providers, but also regulatory agencies in the healthcare sector. Furthermore, SINTEF will apply the best practices for cybersecurity of CMDs in new projects and potentially towards SINTEF customers and partners outside the consortium. In addition, SINTEF will conduct publication and dissemination activities to demonstrate the applicability and benefits of the proposed guidance. We will also further engage with regulatory bodies to identify gaps and recommend measures to address them in their existing guidelines.

Information Catalyst for Enterprise (ICE) and its subsidiary **Information Catalyst (ICS)** is a specialist SME enabling partners and customers to improve their business activities through cutting edge research and innovation, custom software development, and commercial consultancy services. ICE will seek to use the NEMECYS results to in providing consultancy, support and training services in best practice for cybersecurity of CMDs and in IoT domains with similar security requirements.

Ospedale San Raffaele (OSR) is a research institute which is building expertise in cybersecurity by participating in several research projects in the field of cybersecurity. Participating in the NEMECYS project will allow us to become more competitive and appealing for new consortia in the future, which, in turn, will allow us to receive more funding to develop new tools and implement new security measures. Being a private hospital, we take cybersecurity very seriously, and we know it has a significant impact on our reputation. More patients will be drawn to OSR if the hospital is widely known to implement the most up-to-date cybersecurity measures, and this will increase the hospital's revenues. Lastly, we will take the opportunity to improve our current services. For example, we developed a web application that provides nutritional programmes, whose security can be further enhanced by using the results of NEMECYS, which will allow us to integrate new medical devices into the service. Making the solution

more complex and improving its security will make it more valuable on the market, should we decide to sell it in the future.

The **University of Ioannina (UoI)** will utilize the results obtained from the NEMECYS project to drive cutting-edge research initiatives in collaboration with industry partners, academic institutions and other stakeholders. This research will aim to address emerging challenges, identify novel vulnerabilities, and propose effective countermeasures to safeguard the integrity, confidentiality and availability of medical device systems. Furthermore, the UoI recognizes the significance of disseminating knowledge and raising awareness about cybersecurity among the stakeholders. The findings of the project will serve as vital material for lectures, courses and training programs covering a broad range of topics, including secure development practices, threat modelling, vulnerability assessment, incident response planning and regulatory compliance to enhance cybersecurity practices and the protection of patient safety and sensitive data. Overall, the results of the NEMECYS project not only serve as a valuable resource for further research but also provide a foundation for educational initiatives at the UoI.

PD Neurotechnology (PDN) has a NEMECYS exploitation plan with four main pillars:

- *Improve our people*.
  Awareness of all PD Neurotechnology employees in cybersecurity risks, improve the skills and competence of Quality Management and IT department in the utilization of modern risk management tools for evaluating risks (not only cybersecurity ones), improve the skills and competence of R&D staff in the evaluation and assessment of cybersecurity, for all the different technologies applicable in our product development including mobile app development, web development, firmware and hardware. Moreover, participation in project meetings and close collaboration with other partners helps the team build communication and collaboration skills and become familiar with large multi-partner projects. Participation in cybersecurity conferences and events also provides an opportunity for collaborations that could bring additional knowhow to our team.
- *Improve our processes*.
  Update and improve our processes in design and development, risk management, IT and Information Security Management Systems (ISO/IEC 27001), as well as quality management (also for internal/external communication) based on the NEMECYS project results and tools.
- *Improve our products*.
  By improving our people and our design and development process we are going to produce better and safer products. Cybersecurity is becoming a major concern in both Medical Device Regulation (EU) as well as Food and Drug Administration (USA). Moreover, cybersecurity certificates and harmonization to specific guidelines/standards is also essential for specific healthcare systems like the UK National Health Service (NHS). Therefore, cybersecurity awareness and products which are safe by design are essential.
- *Improve our company*.
  Improving people, processes and our products improves ultimately our company. Moreover, participation in large EU projects and the dissemination and exploitation activities involved provides a great opportunity to expand our network and create new business opportunities.

Debiotech (DB) is developing mobile applications which are Software as Medical Device (SaMD). One of these applications will be classified as a IIb medical device, meaning that a misuse of the SaMD could result to the death of the user. To prevent this risk, DB is looking for a solution that will provide a secure and safe environment around these SaMD, which will ensure:

- the confidentiality of the data managed by the SaMD (this includes storage, processing and their transfer to backend servers located in the cloud);
- The integrity of the data managed by the SaMD; and
- The availability of the external services used by the SaMD.

DB wants to use the tools developed in NEMECYS to get this secure and safe environment. They will lead to a protection layer that will be integrated into the SaMD and installed with it.

The NEMECYS project will allow **Mode Sensors (MODE)** to leverage its secure features to position it as a trusted solution in the market. The plan includes four exploitable items.

- *Secure wireless connectivity*.
  The project aims to develop protocols, encryption methods and authentication mechanisms for secure data transmission. The plan involves emphasizing this feature as a unique selling point, targeting healthcare organizations prioritizing data security, and collaborating with wireless technology providers.
- *Data encryption and integrity mechanisms*.
  Encryption and integrity mechanisms will be developed to protect device data. The plan involves ensuring compliance with relevant regulations, building trust through effective communication, and partnering with data security experts for validation and certification.
- *Secure data storage*.
  The project includes developing secure data storage mechanisms. The plan involves communicating the secure data storage capabilities of the device, assuring data privacy and aligning with industry-leading cybersecurity standards.
- *Continuous threat monitoring and response*.
  The project includes developing continuous threat monitoring and response capabilities. The plan includes highlighting proactive threat mitigation, offering security incident response services and collaborating with cybersecurity service providers.

4.2 Exploitable item 2 - Proportionate risk benefit schemes balancing cybersecurity, ethics and clinical benefit – research and tooling

These schemes will enable device manufacturers, system integrators and operators to assess both device and systemic cybersecurity risk proportionate to clinical benefit at design time and runtime for devices and connected scenarios they are deployed in.

SINTEF will exploit risk benefit schemes via CORAS and via publication and dissemination. CORAS is a model-driven risk assessment approach consisting of a customized language for threat and risk modelling, detailed guidelines [14], and an open-source tool [15]. Developments from NEMECYS will advance CORAS to support cyber-risk assessment in the context of connected medical devices, which will be freely available for the benefit of the relevant communities. SINTEF will exploit the results on cyber-risk indicators, threat models, corresponding risk assessment algorithms, and the potential

training material to enhance research priorities and align them with new requirements. SINTEF will exploit innovative results and competences built through the project to promote research and identify strong partners for future opportunities, as well as strengthen and further its position as a leading European actor in the field of cyber risk research.

The **University of Southampton (UoS)** has an open-source community project named SPYDERISK [16] available on GitHub [17] and released under the permissive open-source license Apache 2.0. SPYDERISK is a branded vehicle for the UoS System Security Modeller (SSM) cybersecurity risk assessment toolkit which has been in development for over 8 years and will be enhanced in NEMECYS. UoS will therefore exploit risk benefit schemes via SPYDERISK as community exploitation of the software as a public good and via publication and dissemination. The UoS SSM cybersecurity risk assessment toolkit is a software asset that supports our exploitation aims of creating original research, increasing our reputation via publication and impact creation in communities via SPYDERISK. The SSM consists of a UI, a back-end engine and a knowledge base, and developments from NEMECYS will enhance these components as necessary and appropriate, and will be made publicly available through SPYDERISK. Our expectation is that new knowledge will be created from the analysis of connected medical devices and the trade-off between cybersecurity controls and patient benefit, which will be published and will also enhance the SSM knowledge base, which is available open source for the community via SPYDERISK. Throughout its history the SSM has been evaluated in various trials by end users who have confirmed its benefit in decision support for cybersecurity, and our aim in community development is to create a public good out of the work. To this end, we are actively engaging with the cybersecurity community as potential users of, and contributors to, SPYDERISK. We have strong contacts in the community (e.g. via our connections described in the Annex of NEMECYS D5.1) and we are currently exploring routes and methods for this engagement, with positive results so far.

IBM takes privacy as relevant for both cybersecurity and ethics. IBM's initial exploitation plans are to exploit tooling for risk analysis of Machine Learning models, both within the organization, and as a value added to the Cloud Pak for Data offerings. Some of IBM's analytics will be made available as open source, however some may remain proprietary based on requirements by the IBM business unit that is the recipient of the technology.

Athens Technology Center (ATC) acts as an integrator of healthcare systems and services in research and innovation projects. By implementing risk benefit schemes that balance cybersecurity, ethics and clinical benefit, ATC can benefit in several ways. It can enhance cybersecurity measures to protect sensitive healthcare information, address ethical considerations in the design and implementation of projects, optimize the clinical benefits of solutions, and utilize research and tooling support for risk assessment and mitigation. This approach helps ATC create secure, ethical, and impactful healthcare solutions that improve patient outcomes and healthcare delivery.

PD Neurotechnology (PDN) aims to fully integrate risk benefit schemes in the design and development process of the company.

4.3 Exploitable item 3 - Customized toolbox for MD manufacturers

This toolbox will contain cybersecurity-by-design tools that help CMD manufacturers build security in from inception of their products via updated guidelines, best practice and cybersecurity risk-benefit tooling that identifies vulnerabilities in their devices and enables simulation of their devices in realistic CMD contexts to detect vulnerabilities exposed when their device is used with other devices.

SINTEF will ensure widespread adoption of the customized toolbox for MD manufacturers by utilizing the components from the firmware fuzzing tool and technical know-how acquired in the project to accelerate work in the Horizon Europe project TELEMETRY. TELEMETRY will develop a testing toolkit platform and testing environment for low-cost consumer edge devices, together with a framework for fuzzing IoT devices on cellular networks. Early results from NEMECYS will therefore be a good starting point. Given the novelty of the firmware emulation domain, we will continuously exploit results through publications, discussing how such tools can help cybersecurity researchers. This new knowledge could also be adapted to other domains as well. Additionally, training activities such as workshops will be organized to demonstrate the benefits and usage of the toolbox to manufacturers. We will also collect feedback from users to improve and update the toolbox as needed.

Information Catalyst for Enterprise (ICE) and its subsidiary **Information Catalyst (ICS)** will seek to use the NEMECYS results in providing consultancy, support and training services on a commercial basis for MD manufacturers and for manufacturers of devices used other IoT domains with similar security requirements.

Ospedale San Raffaele (OSR) will exploit this item as described in section 4.1.

As technology provider, **Athens Technology Center (ATC)** can benefit from offering a customized toolbox for cybersecurity to medical device manufacturers. The toolbox will be able to provide tailored solutions and guidelines to enhance the cybersecurity of medical devices throughout their lifecycle. Manufacturers will be able to implement appropriate security controls, ultimately enhancing the overall cybersecurity posture of the medical devices.

Debiotech (DB) expects to use the outcome of NEMECYS to integrate a secure and safe environment for their Software as Medical Device (SaMD). The goal is to deliver this protective layer with the SaMD. It will be installed with the SaMD. This protective layer should protect the SaMD from threads coming from other applications installed in the user's smartphone or from its connection to the cloud. It should also protect the exchanges of data with backend gateways and servers ensuring that no viruses will be introduced in these remote platforms.

PD Neurotechnology (PDN) aims to fully integrate this toolbox in the design and development process of the company.

Mode Sensors (MODE) will integrate the toolbox for MD Manufacturers in the design and development process of the company. Test results from the tools in the toolbox will be used as part of documentation used for submissions to notified bodies as part of approval processes.

4.4 Exploitable item 4 - Customized toolbox for CMD system integrators

This toolbox will enable MDs to be securely connected into connected scenarios with other devices operated by multiple actors, and assessment of system-level cybersecurity with recommendations for controls to reduce risks.

SINTEF aims to use the customized toolbox for CMD system integrators as input for new projects (such as the Horizon Europe project TELEMETRY) which focus on the security of connected devices, thereby contributing to a more security and interconnected ecosystem. Furthermore, SINTEF will offer the toolbox to associated partners and customers, both in the medical domain and in industries with similar challenges, to assist them in implementing new services in a secure and efficient way.

Information Catalyst for Enterprise (ICE) and its subsidiary **Information Catalyst (ICS)** will use the NEMECYS results in providing consultancy, integration, support and training services on a commercial basis for the deployment of CMDs and for deployment in other IoT domains with similar security requirements.

Marina Salud (MS) will exploit this item as described in section 4.1.

Ospedale San Raffaele (OSR) will exploit this item as described in section 4.1.

Athens Technology Center (ATC) acts as an integrator of healthcare systems and services in research and innovation projects. The customised toolbox for CMD System Integrators will enable ATC to deliver secure and innovative healthcare solutions that meet regulatory requirements and instil trust among stakeholders.

4.5 Exploitable item 5 - Customized toolbox for CMD operators

This toolbox will provide valuable guidance on managing various aspects of the procurement process of medical devices, while ensuring compliance with regulatory requirements. It will enable operators to evaluate existing systems and help decide which devices need to be renovated or replaced. Overall, such a customized toolbox will help improve the security of medical devices and enhance patient safety.

SINTEF aims to maximize the impact of the CMD operator toolbox by using it as input to new projects concerned with the cyber security challenges associated with operating medical devices. As the European health sector is undergoing a major digitalization effort, SINTEF will exploit the procurement and compliance tool, as well as the cybersecurity trainings and best practice tools, to support and enhance these efforts, focusing particularly on the Norwegian health sector.

ICE will seek to use the NEMECYS results in providing consultancy, support and training services on a commercial basis for CMD operators and for operators in other IoT domains with similar security requirements.

Marina Salud (MS) will exploit this item as described in section 4.1.

Ospedale San Raffaele (OSR) will exploit this item as described in section 4.1.

As an integrator of healthcare systems and services, **Athens Technology Center (ATC)** can benefit from a customized cybersecurity toolbox designed for connected medical devices operators, such as hospitals and healthcare providers. This toolbox will enable ATC to offer secure and reliable healthcare services to the operators, fostering trust and compliance with regulatory standards.

5 Conclusions

NEMECYS exploitation will be wide-ranging and high impact regarding the enhanced cybersecurity of connected medical devices, and potentially in many other sectors and applications where IoT devices share confidential or sensitive data.

This deliverable has presented the initial exploitation plan for NEMECYS, setting out the exploitation strategies for commercialisation, open source (community exploitation and commercial services), consultancy services, further research, policy making, and education and training. Exploitation policies, pathways and tools established for Horizon Europe have been reviewed and potential benefits for NEMECYS noted. Expected exploitable results have been summarised, and initial exploitation plans for each set out.

6 References

[1] https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf
[2] http://www.netmba.com/marketing/market/analysis/
[3] https://pestleanalysis.com/what-is-pestle-analysis/
[4] https://health.ec.europa.eu/medical-devices-dialogue-between-interested-parties/overview_en
[5] https://op.europa.eu/en/publication-detail/-/publication/e8376eba-5190-11ec-91ac-01aa75ed71a1/language-en/format-PDF/source-244736022
[6] https://ec.europa.eu/research-and-innovation/en/projects/success-stories
[7] https://cordis.europa.eu/
[8] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-dashboard
[9] https://www.horizonresultsbooster.eu/
[10] https://www.innoradar.eu/
[11] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-results-platform
[12] https://intellectual-property-helpdesk.ec.europa.eu/regional-helpdesks/european-ip-helpdesk_en
[13] https://hsbooster.eu/
[14] Lund, M.S., Solhaug, B. and Stølen, K., 2010. Model-driven risk analysis: the CORAS approach. Springer Science & Business Media. https://link.springer.com/book/10.1007/978-3-642-12323-8
[15] https://coras.tools/
[16] https://spyderisk.com/
[17] https://github.com/SPYDERISK