Grant Agreement No.: 101096342
Call: HORIZON-JU-SNS-2022
Topic: HORIZON-JU-SNS-2022-STREAM-B-01-04
Type of action: HORIZON-JU-RIA

Holistic, omnipresent, resilient services
for future 6G wireless and computing ecosystems

D6.3 Final impact creation report and exploitation plan

Revision: v.1.0.

Work package	WP6
Task	Tasks 6.1, 6.2, 6.3, 6.4
Due date	31/12/2025
Submission date	08/02/2026
Deliverable lead	8Bells
Version	1.0
Authors	Nikolaos Androulidakis (8BELLS), Amrita Prasad (MAR), Maria-Chiara Campodonico (MAR) Diego Lopez (TID), Jose Manuel Manjon (TID), Fabrizio Granelli (CNIT), Alessandro Carrega (CNIT), Xavier Masip (UPC), Eva Rodriguez (UPC), Orazio Toscano (ETI), Michalis Danousis (8BELLS), Charalampos Skianis (8BELLS), Panagiotis Gkonis (NKUA), Alexandros Katsarakis (STS), Vito Gianchini (MAR), Alice Piemonti (MAR), Iulisloi Zacarias (TUBS) Stefanos Venios (Suite5), Emilio Garcia (UMU), Anthony Joel Pogo Medina (UMU), Pedro Elisio (EFACEC), Acilia Coelho (EFACEC), Leesa Joyce (HOLO), George Xylouris (ZORTE)
Reviewers	Orazio Toscano (ETI) Xavi Masip (UPC)

Abstract	The HORSE project addresses the increasing complexity of security, privacy, and resilience challenges in emerging 6G networks by proposing an integrated, AI-driven and intent-based security framework. D6.3 presents the final impact creation report and exploitation plan of the HORSE project, summarising dissemination and communication activities, collaboration initiatives, intellectual property management, and exploitation strategies developed throughout the project lifecycle. It provides a comprehensive overview of the project's Background and Foreground assets, identifies Exploitable Results and Key Exploitable Results, and outlines concrete pathways for their post-project exploitation. The document also highlights HORSE's contributions to standardisation bodies, alignment with EU sustainability objectives, and engagement with the Horizon Results Booster programme.
Keywords	Dissemination, IPR, Background, Foreground, Exploitable Results, HRB, Exploitation plans, Standardisation

DOCUMENT REVISION HISTORY

Version	Date	Description of change	List of contributor(s)
V0.1	22/09/2025	1st version of the ToC	Nikolaos Androulidakis (8BELLS)
V0.2	06/10/2025	Finalisation of ToC	Nikolaos Androulidakis (8BELLS), Amrita Prasad (MAR), Jose Manuel Manjon (TID)
V0.3	23/10/2025	BG, FG, ER and KER tables finalised and inserted	Nikolaos Androulidakis (8BELLS), Amrita Prasad (MAR), Maria-Chiara Campodonico (MAR) Diego Lopez (TID), Jose Manuel Manjon (TID), Fabrizio Granelli (CNIT), Alessandro Carrega (CNIT), Xavier Masip (UPC), Eva Rodriguez (UPC), Orazio Toscano (ETI), Michalis Danousis (8BELLS), Charalampos Skianis (8BELLS), Panagiotis Gkonis (NKUA), Alexandros Katsarakis (STS), Vito Gianchini (MAR), Alice Piemonti (MAR), Iulisloi Zacarias (TUBS) Stefanos Venios (Suite5), Emilio Garcia (UMU), Anthony Joel Pogo Medina (UMU), Pedro Elisio (EFACEC), Acilia Coelho (EFACEC), Leesa Joyce (HOLO), George Xylouris (ZORTE)
V0.4	12/11/2025	Exploitation types, pathways and individual exploitation plans finalised and inserted.	Nikolaos Androulidakis (8BELLS), Amrita Prasad (MAR), Maria-Chiara Campodonico (MAR) Diego Lopez (TID), Jose Manuel Manjon (TID), Fabrizio Granelli (CNIT), Alessandro Carrega (CNIT), Xavier Masip (UPC), Eva Rodriguez (UPC), Orazio Toscano (ETI), Michalis Danousis (8BELLS), Charalampos Skianis (8BELLS), Panagiotis Gkonis (NKUA), Alexandros Katsarakis (STS), Vito Gianchini (MAR), Alice Piemonti (MAR), Iulisloi Zacarias

			(TUBS) Stefanos Venios (Suite5), Emilio Garcia (UMU), Anthony Joel Pogo Medina (UMU), Pedro Elisio (EFACEC), Acilia Coelho (EFACEC), Leesa Joyce (HOLO), George Xylouris (ZORTE)
V0.5	10/12/2025	Content around JOAs, HRB and contributions to EU sustainable Goals finalised and inserted.	Nikolaos Androulidakis (8BELLS), Amrita Prasad (MAR), Maria-Chiara Campodonico (MAR) Diego Lopez (TID), Jose Manuel Manjon (TID), Fabrizio Granelli (CNIT), Alessandro Carrega (CNIT), Xavier Masip (UPC), Eva Rodriguez (UPC), Orazio Toscano (ETI), Michalis Danousis (8BELLS), Charalampos Skianis (8BELLS), Panagiotis Gkonis (NKUA), Alexandros Katsarakis (STS), Vito Gianchini (MAR), Alice Piemonti (MAR), Iulisloi Zacarias (TUBS) Stefanos Venios (Suite5), Emilio Garcia (UMU), Anthony Joel Pogo Medina (UMU), Pedro Elisio (EFACEC), Acilia Coelho (EFACEC), Leesa Joyce (HOLO), George Xylouris (ZORTE)
V0.6	31/12/2025	HRB section finalised and inserted, exploitation part completed	Nikolaos Androulidakis (8BELLS)
V0.7	23/01/2026	Dissemination and standardisation parts completed	Amrita Prasad (MAR), Maria-Chiara Campodonico (MAR) Diego Lopez (TID), Jose Manuel Manjon (TID)
V0.8	27/01/2026	Draft ready for review	Nikolaos Androulidakis (8BELLS), Amrita Prasad (MAR), Maria-Chiara Campodonico (MAR) Diego Lopez (TID), Jose Manuel Manjon (TID)
V0.9	29/01/2026	The review process completed and updates done based on the reviewer's comments	Nikolaos Androulidakis (8BELLS), Amrita Prasad (MAR), Maria-Chiara Campodonico (MAR) Diego Lopez (TID), Jose Manuel Manjon (TID), Orazio Toscano (ETI), Xavi Masip (UPC)
V1.0	08/02/2026	Final check and submission	Fabrizio Granelli (CNIT)

Disclaimer

Copyright notice

Project co-funded by the European Commission in the Horizon Europe Programme		
Nature of the deliverable:	R	
Dissemination Level		
PU	*Public, fully open, e.g. web*	**X**
SEN	*Sensitive, limited under the conditions of the Grant Agreement*	
Classified R-UE/ EU-R	*EU RESTRICTED under the Commission Decision No2015/ 444*	
Classified C-UE/ EU-C	*EU CONFIDENTIAL under the Commission Decision No2015/ 444*	
Classified S-UE/ EU-S	*EU SECRET under the Commission Decision No2015/ 444*	

* *R: Document, report (excluding the periodic and final reports)*
DEM: Demonstrator, pilot, prototype, plan designs
DEC: Websites, patents filing, press & media actions, videos, etc.
DATA: Data sets, microdata, etc
DMP: Data management plan
ETHICS: Deliverables related to ethics issues.
SECURITY: Deliverables related to security issues
OTHER: Software, technical diagram, algorithms, models, etc.

Executive summary

The document at hand, developed in the context of WP6, builds upon what has been outlined in D6.2 (Impact Creation Report and Exploitation Strategy V1.0). The document serves the main purpose of offering an in-depth report on the project's communication, dissemination, Intellectual Property Rights (IPR) exploitation, standardisation and community-building strategy that has been developed in the 2nd half (final phase) of the project. The dissemination, communication and community-building strategy has been followed by all project partners to maximize the impact of HORSE project and ensure that the following communication-related project objectives are met:

- Ensure HORSE's broad visibility by spreading knowledge about project activities and its results.
- Reach, stimulate, and engage a critical mass of relevant stakeholders to ensure that the project results are effectively showcased, leading to widespread validation, improvement, and further adoption of the developed technologies and concepts.
- Facilitate exploitation of project outcomes and promote the development of innovative solutions based on the HORSE technologies and architecture.
- Foster an impactful contribution to relevant standardization bodies.
- Ensure close coordination with the SNS community and establish liaisons with relevant initiatives, such as 6G-IA, SNS-JU, etc.

Besides describing the communication, dissemination, and community-building activities conducted by the HORSE consortium during M19-M36 of the project, D6.3 presents actions taken to address recommendations offered during the previous project review, plans of activities after the project's end, and an overview of standardization and exploitation activities carried out by the project partners. More specifically, a key focus of this report is the systematic management of IPR during the second implementation period of the project. The document clearly distinguishes between Background (BG) and Foreground (FG) intellectual assets and presents the HORSE Innovations, Exploitable Results (ERs), and Key Exploitable Results (KERs) identified by the consortium. For each result, ownership propositions, protection mechanisms and licensing models are defined.

Building upon this structured IPR framework, the deliverable outlines concrete exploitation pathways tailored to the objectives and profiles of individual partners. These pathways span research continuation, industrial integration, commercialisation, and standardisation-driven adoption. D6.3 also documents the consortium's engagement with the Horizon Results Booster (HRB) programme, which supported the refinement of value propositions, exploitation strategies, and business planning for selected results.

Finally, the deliverable highlights HORSE's contributions to relevant standardisation bodies and its alignment with the United Nations Sustainable Development Goals, reinforcing the project's commitment to responsible innovation and long-term societal impact.

Table of contents

List of figures

List of tables

Abbreviations

AI	Artificial Intelligence
BG	Background technology
CAS	Compliance Assessment
DFF	Data Fusion Framework
DOC	Domain Orchestrator Connector
DTE	Distributed Trustable AI Engine
EC	European Commission
EM	Early Modelling
ePEM	End to end Proactive Secure Connectivity Manager
ER	Exploitable Result
ETSI	European Telecommunications Standards Institute
FG	Foreground Technology
G2M	Go-to-Market
GA	Grant Agreement
HRB	Horizon Results Booster
IBI	Intent-based Interface
IETF	Internet Engineering Task Force
IPR	Intellectual Property Rights
IRO	Intent-based Resilience Orchestrator
JOA	Joint Ownership Agreement
KER	Key Exploitable Result
LLM	Large Language Model
ML	Machine Learning
NDT	Network Digital Twin
NFVCL	Network Function Virtualisation Convergence Layer
OSM	Open-Source MANO
OSS	Operations Support System
PAG	Policies and Data Governance
PEI	Potential Exploitation Interest
PEM	Predictive Engine and Mitigation
PM	Person-Month
RTR	Reliability Trustworthiness Resilience
SDG	Sustainable Development Goal

SM	Smart Monitoring
SME	Small Medium Enterprise
SNS	Smart Network and Services
SWOT	Strengths, Weaknesses, Opportunities, Threats
TRL	Technology Readiness Level
UN	United Nations
UVP	Unique Value Proposition
XR	Extended Reality

1 Introduction

The rapid evolution of communication networks towards highly programmable, AI-driven, and service-oriented architectures is a defining characteristic of future 6G ecosystems. While these developments enable unprecedented levels of flexibility, efficiency, and performance, they also introduce significant challenges related to security, privacy, trustworthiness, and resilience. The increasing reliance on software-defined infrastructures, distributed intelligence, and automated decision-making mechanisms expands the attack surface and amplifies the potential impact of cyber threats across critical digital services and infrastructures.

In this context, the HORSE project was initiated with the objective of designing and validating an integrated security framework capable of addressing the complex and dynamic threat landscape of 6G networks. HORSE adopts a holistic approach that combines intent-based management, artificial intelligence, network digital twins, and secure orchestration mechanisms to enable proactive, adaptive, and automated security operations.

D6.3, the Final Impact Creation Report and Exploitation Plan, consolidates the outcomes of the HORSE project from an impact, dissemination, and exploitation perspective. It builds upon previous impact creation reports by presenting a complete and final overview of the activities carried out, the results achieved, and the strategies defined to ensure the sustainability and uptake of project outcomes after the project's conclusion.

A central element of this report is the systematic assessment of HORSE's intellectual assets. The document identifies and classifies the BG and FG technologies developed or utilised within the project and highlights the innovations that form the foundation for exploitation activities. Based on defined qualitative and quantitative criteria, the consortium has identified a set of ERs and KERs, each accompanied by clear ownership propositions, protection schemes, and licensing models.

In parallel, the report documents the extensive communication and dissemination activities undertaken to maximise the visibility and impact of HORSE results including scientific publications, participation in major international events, contributions to white papers and standardisation efforts, and engagement with the broader SNS ecosystem. Special emphasis is placed on aligning technical innovation with market needs and societal priorities, including sustainability, trust, and regulatory compliance.

To sum up, D6.3 can provide a clear roadmap for the continuation and adoption of HORSE results, ensuring that the project's contributions will extend well beyond its funded lifetime.

2 Dissemination and Communication

Communication and dissemination activities are central to the overall HORSE effort. They are being closely monitored and coordinated to ensure an effective engagement of all targeted stakeholders, including those in the broader 6G, privacy and cybersecurity ecosystems and related vertical domains. To raise awareness and maximize the impact of the project, a comprehensive communication and dissemination plan was developed in Q1 of the project (see D6.1 for details). In the next version of this document, D6.2 (Impact Creation Report and Exploitation Strategy V1.0), the document reported the activities carried out in the first half of the project, from M1-M18.

The execution of a solid communication and dissemination plan began at the early project stages and continued at steady pace throughout the entire lifecycle of the project. Building upon the activities outlined in the Impact Creation Report and Exploitation Strategy (D6.2), a set of dedicated online and offline activities, outlined below, has been pursued to support the achievement of project objectives and ensure a broad promotion and effective showcasing of developed concepts, technologies, use cases, and project results. These activities are conducted under MARTEL's leadership and guidance with active contributions from all HORSE project partners.

WP6 leads a set of dedicated dissemination and communication actions with the following objectives:

- Ensure broad visibility and awareness of HORSE, promoting project knowledge and establishing a recognizable identity to support promotional and marketing efforts.
- Engage and stimulate a critical mass of relevant stakeholders to effectively showcase project results, leading to validation and further adoption of the developed technologies.
- Contribute significantly to relevant scientific domains and standardization bodies as appropriate and relevant to planned exploitation plans and project outcomes.
- Establish liaisons and ensure close collaboration with relevant initiatives in the industry and R&I domains, particularly those launched as a result of the SNS joint undertaking, other similar initiatives, and projects being funded in the SNS stream B.

In the final reporting period, dissemination and communication activities were carried out related to the second and third phases of communication and dissemination activities, as defined in D6.1 and D6.2. All the above actions are depicted in Figure 1.

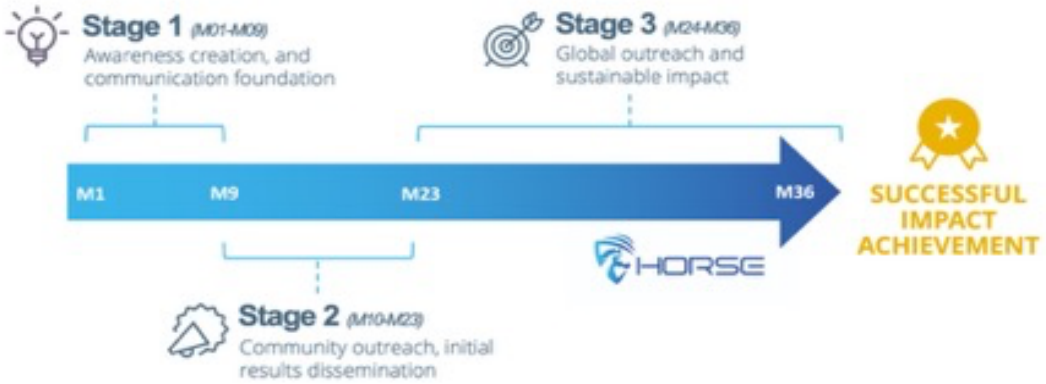


Figure 1: HORSE Impact Creation phases

During this final phase of the project, the main focus has been to amplify the outputs and results of the project. The consortia engaged with the target stakeholders and presented the

results and know-how developed from the project. The following dissemination strategy and activities were carried out:

- Organizing the Privacy workshop at the CAMAD 2024 conference: HORSE project organized a day long workshop at the CAMAD 2024 conference where the main scope of the workshop was to discuss the privacy and cybersecurity challenges in 6G. HORSE invited intervention from other SNS Stream B projects like, the HEXA-X project, RIGOUROUS and PRIVATEER. This exchange of know-how, challenges and innovations was very fruitful in showcasing the advancements in 6G cybersecurity in Europe.
- Presenting project results: HORSE showcased the initial outcomes and milestones at various events and conferences.
- Producing videos to raise awareness: Several promotional videos were created to highlight the project's objectives, achievements, impact as well as use case demo to show the real-time application of HORSE technology.
- Animating social media channels: The project team actively engaged with stakeholders and the public through various social media platforms.
- Publishing news items on the project website and media: Regular updates were posted to keep stakeholders informed about the project's progress.
- Distributing newsletters: Periodic newsletters were sent out to stakeholders to maintain interest and update them on project milestones.
- Participating in events: Team members attended events to network, share knowledge, and promote the project.

2.1 Communication and Dissemination Activities M19-M36

2.1.1 Project website

The HORSE website www.horse-6g.eu (see Figure 2), is the main information hub presenting the project’s goals, activities, achievements, outputs and resources. The website was launched in January 2023 at the time of the official start of the project and features the following:

- General information about the project, its vision, objectives, and anticipated impact.
- Information about project use cases and enabling functions.
- A brief introduction to all members of the consortium.
- News items and press releases.
- List of relevant events.
- A repository of resources, such as scientific publications, presentations/talks, promotional materials, videos, and public deliverables.
- Contact forms and information.
- An acknowledgment and reference to the Smart Networks and Services Joint Undertaking of the European Union’s Horizon Europe Research and Innovation programme.

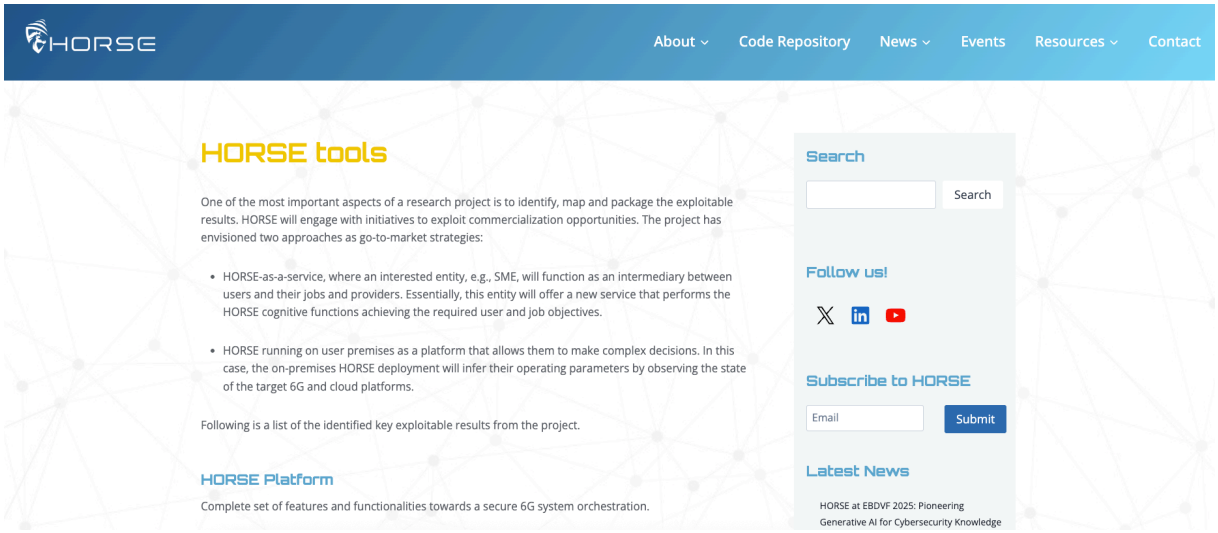


Figure 2: The HORSE Website

The website has been periodically updated during the evolution of the project.

In terms of reach/engagement, in the reporting period, the website counts **3508 unique visitors**, that have generated 5888 page views and an average visit duration of about **1 min and 30 seconds** as shown in Figure 3.

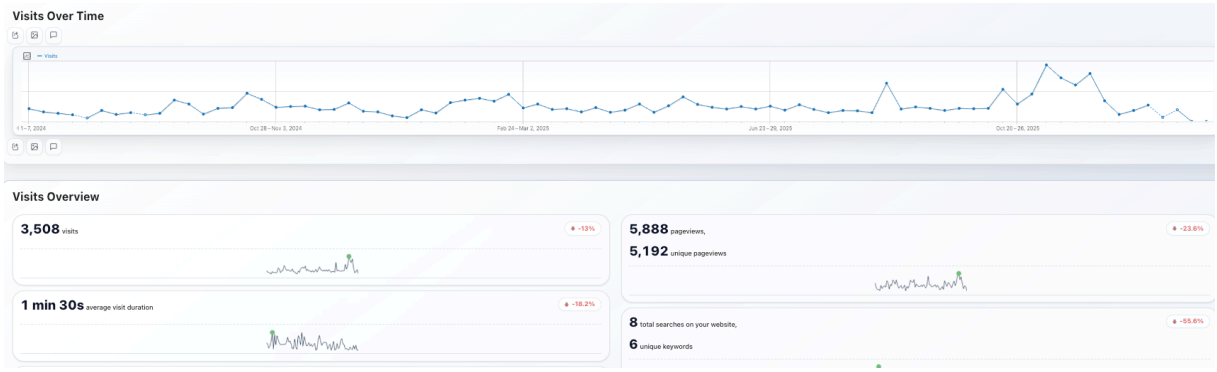


Figure 3: HORSE website visitor's log

The following figures (Figure 4 and Figure 5), show the visitor's demographics. The visitors of the HORSE website are in all areas of the world.

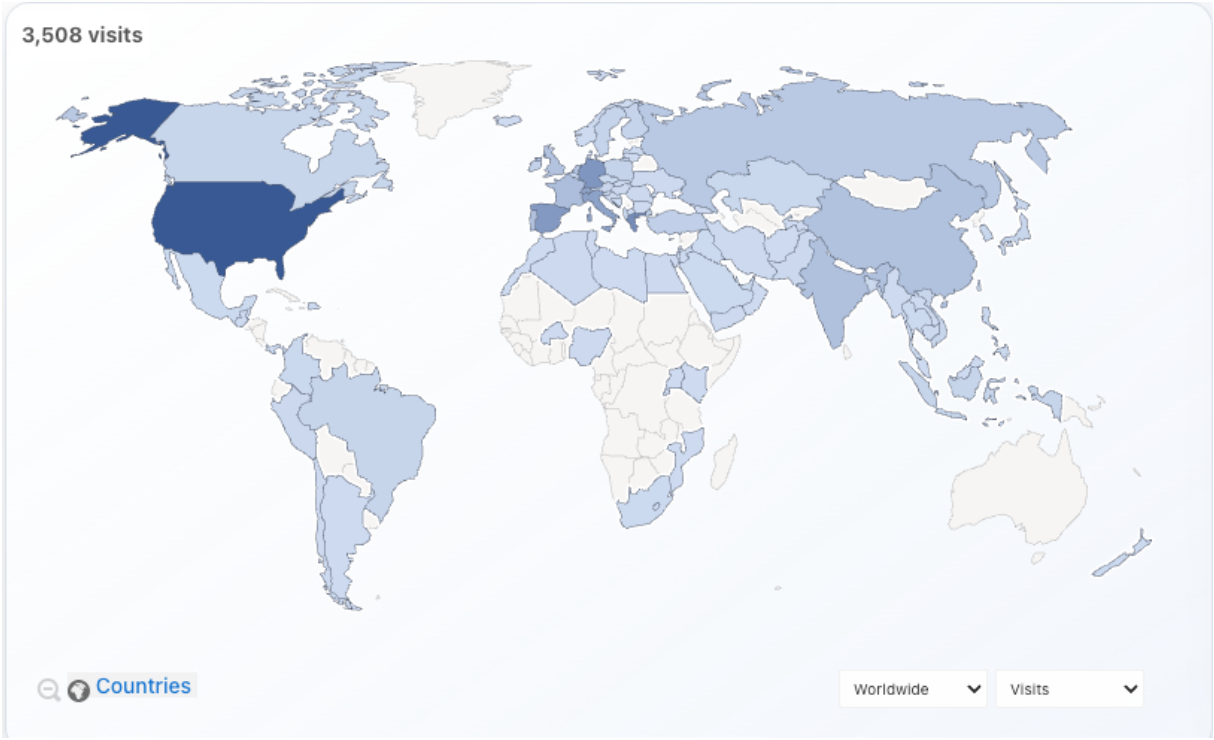


Figure 4: Geographical distribution of HORSE website visitors

Figure 5 shows the top 5 countries from where most of the visits have been made on the website.

Country

COUNTRY	VISITS
United States	604
Greece	355
Germany	310
Spain	294
Italy	256

1–5 of 97 Next ›

5

Figure 5: HORSE website visitors: top 5 countries

Figure 6 shows the most visited pages on the HORSE website.

Pages

PAGE URL	PAGEVIEWS	UNIQUE PAGEVIEWS
/index	2,419	2,064
event	558	495
consortium	398	353
deliverables	296	277
latest-news	237	192
all-events	165	143
use-cases	145	133
horse-tools	131	120
presentations	133	119
publications	131	111
contact	107	104
anomaly-detection-and-mitigation-in-6g-networks-via-machine-learning	117	102
advisory-board	97	85
videos	87	81

Figure 6: HORSE website's most visited pages

The most visits, seen in Figure 5, are from the USA, Greece, Germany, Spain and Italy. This reflects, in part, the composition of the consortium and the communication activities undertaken by partners, as well as the participation in international conferences, events and workshops.

Based on the provided analytics data for the HORSE website for the period of July 2024 to Dec 2025, we have the following traffic sources:

Direct: 2104 visits (60%): Direct traffic occurs when users type the website's URL directly into their browser's address bar, access it through browser bookmarks, or click on a link in an email or a document (e.g., a PDF). This traffic source often reflects users who are already familiar with the project or have visited the website before.

Search Engines: 1169 visits (33%): Organic search traffic refers to users who found website through a search engine (e.g., Google, Bing, Yahoo) by entering relevant keywords.

Referral: 153 visits (4%): Referral traffic is generated when users visited the website by clicking on a link from another website. This could include links in blog posts, news articles, or online directories.

Social: 66 visits (2%): Social traffic comes from users who find and visit the website through social media platforms (e.g., Facebook, Twitter, LinkedIn, Instagram).

All information and e-mails collected are protected under the General Data Protection Regulation (GDPR). Contact was only made with people who submitted inquiries. Similarly, the newsletters were sent out only to individuals who have explicitly requested to receive them. The website provides information on the data kept and how they are used in alignment with the GDPR under the Privacy policy link (footer of the webpage).

Last but not the least, HORSE opted for an environmentally responsible website hosting platform, which has been designed to be as energy efficient as possible to limit the unnecessary waste of resources. The web hosting provider, GreenGeeks, puts back three times the power consumed into the grid in the form of renewable energy.

2.1.2 Social media channels

HORSE established its presence on social media channels to regularly promote project activities and outputs while encouraging a wider discussion on topics related to 6G research and deployment as well as topics like AI/ML, cybersecurity, privacy, digital twinning, etc. The project has built a fair follower base on the prominent social media channels, namely X and LinkedIn which are all linked to the project's website.

For most of the promotional posts, social media cards are created following the brand identity of the project and these social media cards are used for the promotion of project events, international days of relevance, newsletter announcements etc. Some examples of social media cards (Figure 7) produced for HORSE project are:

Figure 7: HORSE social media cards

2.1.2.1 X (Formerly Twitter)

HORSE uses X, as a dynamic social network covering the news in real-time at a global level. To date, the HORSE Twitter account (@HORSEProjectEU) has attracted **294 followers**. The project follows 139 accounts, mostly projects and initiatives in similar fields. The project's X account is used predominately to promote and disseminate project activities and developments but also to learn about and cross-share relevant and interesting events and initiatives, and to establish meaningful connections with relevant stakeholders, including policy makers, industry, and the general public (Figure 8).

Figure 8: HORSE X account

2.1.2.2 LinkedIn

LinkedIn, as one of the biggest business networks in the world (over 150 million users in more than 200 countries and territories), is a useful tool for HORSE. It allows the project to network with individuals and organizations within the industry and beyond, share relevant information about project activities, and stay up to date on the latest developments in the field. To date, the HORSE LinkedIn account (horse-project-eu) has attracted **509 followers**. Similar to X, the LinkedIn account is used to promote project activities and learn about and cross-share relevant events and activities. Figure 9 presents the project's LinkedIn profile.

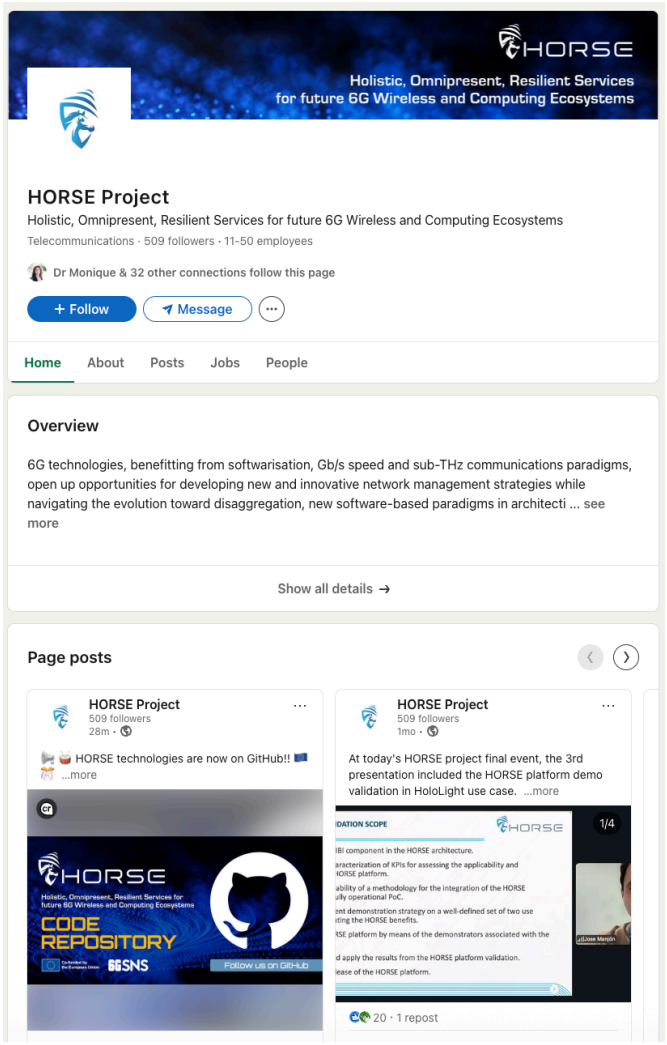


Figure 9: HORSE LinkedIn page

2.1.3 News items, press releases

The HORSE consortium keeps the community and the general public informed about relevant activities, undertakings, and events by publishing news items and press releases. To date, **28 news items and 2 press releases** have been published on the project website.

The consortium has an effective way of generating technical content from the project. The consortium produces a blogpost per month which a partner has to provide. The idea of the blogpost is about a technical in depth writeup about a technology or a concept that is useful to the HORSE and 6G community. So far **11 technical blogposts** have been published from the consortium.

Figure 10 shows the news items and blogposts published on the website.

Figure 10: HORSE project news page

2.1.4 Newsletters

The HORSE periodic newsletter is sent out twice a year, providing updates on the 6G, privacy and cybersecurity ecosystems, as well as on the project activities, findings, and results. The project newsletters also contain information on the upcoming tasks, events, as well as any relevant news and announcements from individual project partners when relevant. A mailing list based on subscription has been created, giving the possibility to share the newsletter via mass mailing. A registration functionality allowing interested visitors to subscribe to the newsletter has been available on the project website since the beginning of the project. The design of each newsletter is aligned with the HORSE brand identity. The newsletter is also fully responsive to ensure its readability on any device.

All issued newsletters are being uploaded on the website (available at https://horse-6g.eu/newsletter/) upon their distribution to subscribers. To date, **6 newsletters** have been sent out. In Appendix A – HORSE latest newsletter the latest newsletter can be found.

2.1.5 Publications

The HORSE consortium is committed to bringing research results closer to the public and adheres to the Open Access guidelines set by the Horizon Europe work programme. All project partners are strong supporters of Open Access as it enables all interested parties to use published research results irrespective of their location or income, boosting the transfer of knowledge between science, the economy, and society at large. The project has been very active in that sphere since its early stages. The below Table 1 lists all the accepted/published papers stemming from HORSE in this reporting period.

Title of the paper	Authors	Conference/Journal
A differential privacy protection-based federated deep learning framework to fog-embedded architectures	Gutierrez, N.; Otero, B.; Rodriguez, E.; Utrera, G.; Mus, S.; Canal, R.	Journal of Engineering applications of artificial intelligence
A Distributed Approach for Detecting and Mitigating DDoS Attacks on White-Boxes	Pablo Armingol Robles, Juan Carlos Caja Diaz and Antonio Agustin Pastor Perales	Silicon Valley Cybersecurity Conference (SVCC 2023). IEEE
ePEM: an End-to-End Proactive Secure Connectivity Managerfor 6G Orchestrator Solutions	Alessandro Carrega, Ramin Rabbani	2024 IEEE CAMAD Conference. IEEE
System Level Performance Assessment of Large-Scale Cell-Free Massive MIMO Orientations With Cooperative Beamforming	Panagiotis K. Gkonis, Spyros Lavdas, George Vardoulias, Panagiotis Trakadas, Lambros Sarakis and Konstantinos Papadopoulos	IEEE Access
Optimizing Network Cybersecurity: AI-Powered NLP for Natural Language Command Interpretation	Michalis Danousis, Konstantinos Kaltakis, Alexandros Dimos, Charalabos Skianis, Emmanouil Kafetzakis, Ioannis Giannoulakis	2024 IEEE CAMAD Conference. IEEE
A Security Services Management Architecture Toward Resilient 6G Wireless and Computing Ecosystems	Eva Rodriguez, Xavi Masip-Bruin, Josep Martrat, Rodrigo Diaz, Admela Jukan, Fabrizio Granelli, Panagiotis Trakadas and George Xilouris	IEEE Access
Strategy for Modeling Threats in 5G and B5G Networks	Saman Tariq, Eva Rodriguez, Xavi Masip, Panos Trakadas, Admela Jukan and Diego R.Lopez	SioTec - CCGRID 2024 Conference. IEEE
Revolutionizing Cloud Security with Programmable Frameworks: a Novel Approach	Alessandro Carrega	IEEE FNFW2024
Organizing and augmenting cybersecurity knowledge using generative AI	Alice Piemonti, Vito Cianchini, Michail Danousis, Harry Skianis	IEEE 11th International Conference on Network Softwarization (NetSoft)
Securing 6G Networks: the HORSE Approach Using LLM-Driven Mitigation Actions	M. Danousis, A. Piemonti, F. Granelli, X. Masip-Bruin, E. Rodriguez, A. Carrega, C. Skianis, E. Kafetzakis, I. Giannoulakis	EuCNC 6G Summit 2025
Navigating the Cybersecurity Landscape in Cloud	M. Akbari, R. Bruschi, A. Carrega	International Conference on Communications,

Computing: Challenges, Strategies, and Future Directions		Computing, Cybersecurity, and Informatics (CCCI)
Enhancing 6G Network Resilience through HORSE's LLM Agent-Based Security Mechanisms	M. Danousis, A. Piemonti, F. Granelli, X. Masip-Bruin, E. Rodriguez , A. Carrega, H. Skianis, E. Kafetzakis, I. Giannoulakis	2025 IEEE Global Communications Conference
B5G/6G Cyber Security Testbed	A. Carrega, F. Davoli, R. Rabbani	IEEE Way to 6G Workshop at MASCOT 2025
On Effectiveness of Graph Neural Network Architectures for Network Digital Twins (NDTs)	I.Zacarias, O. B. Taarit, A.Jukan	IEEE Conference on Network Function Virtualization and Software-Defined Networking (NFV-SDN)
A Survey on 5G Private and B5G Network Threats and Safeguarding AI-based Security Mechanisms through the Layered Analysis	Saman Tariq, Eva Rodriguez Luna, Xavier Masip Bruin, Rodrigo Diaz, Josep Martrat, Panagiotis Trakadas	Computer Networks
5G Penetration Testing as a Service	A. Carrega	9th Cyber Security in Networking Conference (CSNet) - Demo & work in progress papers
Enhancing cybersecurity in railways: Machine learning approaches for attack detection	Calviño, B. O., Rodriguez, E., Costa, J. J., & Oriol, M.	International Journal of Critical Infrastructure Protection
Federated Transfer Learning-based Intrusion Detection System in 5G networks	Bellmunt, A., Otero, B., Rodriguez, E., Masip-Bruin, X.	Expert Systems with Applications

Table 1: HORSE scientific publications

2.1.6 Project videos

The HORSE project has a YouTube channel for its videos. **11 videos** have been published on the website, including the Project Overview video, use-case demos and interviews covering specific topics relevant to the HORSE project.

Figure 11 below shows the HORSE project YouTube channel.

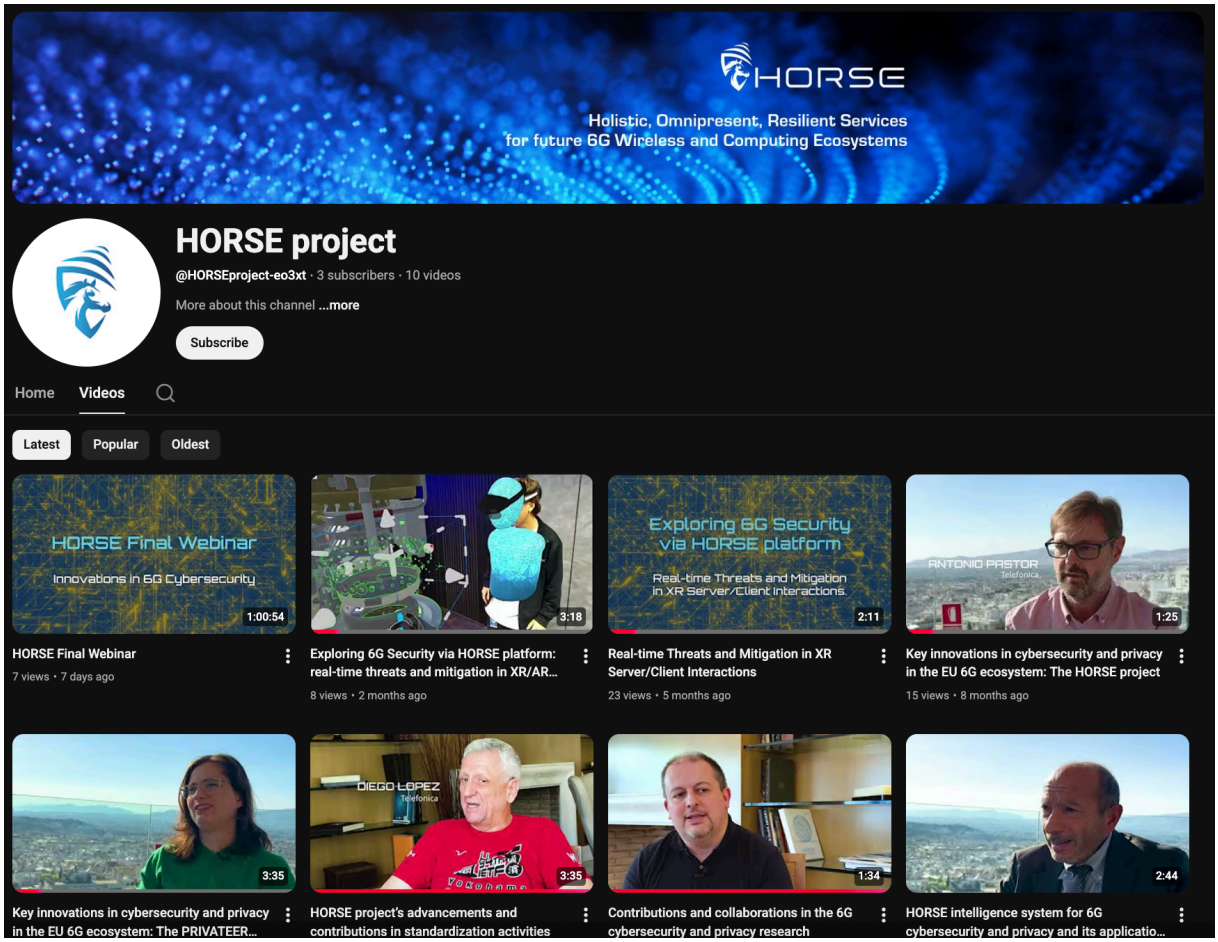


Figure 11: HORSE YouTube channel

2.1.7 Digital and printed promotional materials

The HORSE project partners have participated in many events during the course of the project and have carried with them the different promotional materials that were produced. We have also participated in conferences with poster presentation. All promotional artefacts of the project has been published on the website (https://horse-6g.eu/promo-materials/).

HORSE also produced event specific promotional material, for example, at the demo presentation at EuCNC 2025, a demo specific flyer was created showcasing the real-time threat mitigation in AR/XR environment.

Figure 12 and Figure 13 show the artifacts created for EuCNC 2025.

Figure 12: HORSE demo flyer for EuCNC 2025

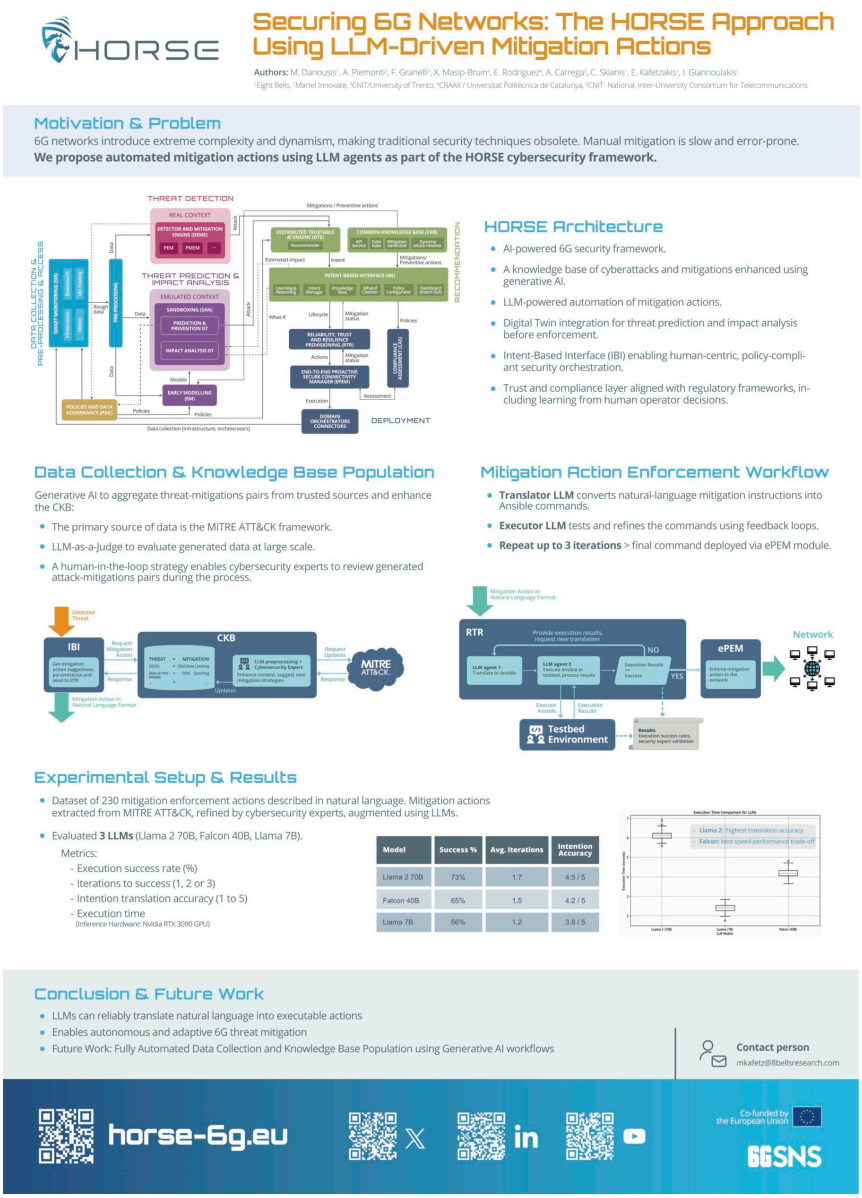


Figure 13: HORSE poster for EuCNC 2025

All promotional materials are printed as well as uploaded on the website.

2.1.8 Events

Event organization and attendance are an important aspect of the HORSE communication and dissemination strategy. Since the project kicked off in January 2023, HORSE coordinator and project partners have taken a very proactive step in raising awareness about the project in the European and global 6G community.

Table 2 provides further details on attended events for the reporting period.

Name of the event	Date, Location	Event website	Type of contribution	Partners involved
Infocom World 2023	Athens, 12/14/2024	https://infocomworld.gr/25o-synedrio-infocom-world-2023-diginvest-in-greece-new-horizons/epistimoniki-enotita-programma/	Presentation	8BELLS
2023 IEEE Future Networks World Forum (FNWF'23)	13-15 November 2023, Baltimore, MD, USA	https://fnwf2023.ieee.org/call-for-proposals/call-workshop-proposals	Workshop organization and panel	UMU
2024 IEEE Future Networks World Forum (FNWF'24)	15–17 October 2024 Dubai, UAE	https://fnwf2024.ieee.org/second-workshop-beyond-current-5g-architecture-6g-service-and-international-cooperation	Workshop organization and panel	UMU
6G Expert Days	08. – 09. April 2024 Munich, Germany	https://5g.nrw/6g-expert-days-2024/	Panel	HOLO
11th ANACOM Conference	10-11 Sept2024, Lisbon	https://anacom.pt/render.jsp?categoryId=431446	Presentation	Efacec
DigiTwin 2024	14-16 October 2024	http://www.dtiac.com/	Presentation	TID
CAMAD 2024 IEEE International Workshop on Computer-Aided Modeling and Design of Communication Links and Networks (CAMAD)	21-23 Oct 2024, Athens	https://camad2024.ieee-camad.org/program/workshops	Presentation	8BELLS
Addressing 6G Cybersecurity and Privacy Challenges, CAMAD 2024, Workshop	23 Oct 2024, Athens	https://camad2024.ieee-camad.org/program/workshops	Workshop organization and panel	All partners
ETSI AI Conference - How Standardization	10-12 Feb 2025, Sophia Antipolis	https://www.etsi.org/events/2451-etsi-ai-conference-2025	Presentation	TID, Martel

is Shaping the Future of AI				
IEEE ICC 2025	8-12 June 2025, Montreal	https://icc2025.ieee-icc.org/workshop/ws14-second-workshop-path-towards-6g-standardization-and-research-vision	Workshop organization	CNIT
EuCNC 2025	3-6 June, Poznan	https://www.6gflagship.com/event/eucnc-6g-summit-2025/	Demo, poster, panel, presentation	Martel, HOLO, CNIT, 8Bells
IEEE 11th International Conference on Network Softwarization (NetSoft)	23-27 June 2025, Budapest	https://ieeexplore.ieee.org/document/11080630	Presentation	Martel, 8bells
IEEE WT6G at MASCOTS	21-23 October 2025, Paris	https://www.telecomtv.com/content/dsp-leaders-forum-agenda-day-2/	Presentation	CNIT
ETSi Security Conference 2025	6-9 Oct 2025, Sophia Antipolis, France	https://www.etsi.org/events/2481-etsi-security-conference-oct2025#pane-7/?jjj=1758032518099	Demo booth	CNIT, HOLO
9th Cyber Security in Networking Conference (CSNet) - Demo & work in progress papers	20 – 22 October, 2025, Abu Dhabi	https://csnet-conference.org/2025	Poster Presentation	CNIT
International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI)	October 15-17, 2025, Hangzhou, China	https://ccci.udg.edu	Presentation	CNIT
European Big Data Value Forum 2025	12-14th November 2025, Copenhagen	https://european-big-data-value-forum.eu/2025-edition/programme/?edition_session_id=14470	Presentation	Martel
ETSI ZSM	25-27 November 2025. Granada, Spain	https://etsiit.ugr.es/en/node/827	PoC	TID

ETSI ZSM Conference at Universidad de Granada (UGR)	26 November. Granada, Spain	https://etsiit.ugr.es/la-escuela/noticias/visitas-la-etsi-zero-touch-network-and-service-management	Presentation	TID
GlobeCom 2025	8–12 December 2025, Taipei, Taiwan	https://globecom2025.ieee-globecom.org/program	Presentation	CNIT
HORSE Final webinar	4th Dec 2025, Online	https://horse-6g.eu/event/horse-final-event/	Webinar organiser	All partners
Architecting trust in 6G: Technical insights from SNS JU Projects	5th Dec 2025, Online	https://smart-networks.europa.eu/architecting-trust-in-6g-technical-insights-from-sns-ju-projects/	Presentation	CNIT

Table 2: HORSE Events overview

3 Collaboration and liaisons with other projects and initiatives

3.1 Liaisons within the SNS-JU landscape

As part of the Task 6.2, HORSE's goals have been to create synergies with other initiatives. To this end, we have reached out to various SNS projects in the Stream B, and the European 5G/6G community, informing them about HORSE's aims and objectives and inviting them to share information on their project with us, in the context of events, panels, scientific workshops, contribution to white papers etc. The objective for creating these connections is to facilitate a cross dissemination of both actions via shared-blog entries, cross-referral on the project websites, mutual social network interaction and event sharing perspective and to have a constant flow of communication between the initiatives in order to promote additional points for collaboration which may emerge in the short and mid-term. Martel, leading the communication dissemination and community building task participates in the monthly SNS JU communication task force calls where updates from the project are shared as well as information about events, CFPs, news items, blogposts etc.

HORSE has regularly participated in the SNS and 6G-IA working groups as well as standardization bodies like ETSI and have contributed to the development of some white papers. Following is a list of the published white papers where HORSE have contributed.

- **6G Security And Trust: Insights From European SNS-JU Projects** - https://6g-ia.eu/wp-content/uploads/2025/11/6g-ia_security-wg_white-paper_nov25_final.pdf
- **6G SNS – 6G for Media and Entertainment** - https://smart-networks.europa.eu/wp-content/uploads/2025/12/white-paper-6g-for-me-v1.0.pdf
- **AI Technologies in Experiential Networked Intelligence to Increase Autonomous Operation** - https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-WP-64-AI_Technologies_in_ENI_to_Increase_Autonomous_Operation.pdf
- **European vision for the 6G Network System** - https://6g-ia.eu/wp-content/uploads/2024/11/european-vision-for-the-6g-network-ecosystem.pdf
- **AI Technologies in Experiential Networked Intelligence to Increase Autonomous Operation** - https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-WP-64-AI_Technologies_in_ENI_to_Increase_Autonomous_Operation.pdf

4 Impact assessment

4.1 Communication and dissemination KPIs

The following metrics in Table 3, are used to monitor and assess the progress of the communication and dissemination activities and provide some measurable outcomes related to their impact created (as far as this is feasible from a quantitative point of view).

Tool/activity	KPI	Target value	Total M1-M36
Website	Unique visitors average (yearly)	>3000	7635
Social media	Number of followers (by project end) on Twitter Number of followers (by project end) on LinkedIn	500 150	294 510
White papers	Number of published white papers	3	3
News items on website	Number of published news items	≥ 20	28
e-Newsletters	Number of newsletters sent out	6	6
Flyers/Brochures Presentations Posters/Roll-Ups	Number of flyers/brochures (incl. digital brochures) Number of project presentations Number of produced posters/roll-ups	3 6 3	3 8 3
Videos	Number of produced videos	6	11
Workshops	Number of attended/organized workshops	3	5
Webinars, panels, demos	Webinars Panels Demos	3+ 3+ 3+	4 5 3
Trainings (online/in-person)	Number of courses offered	2	1
Scientific publications	Number of publications	15+	26
Participation in events & presentations	Number of external events partners attended to promote the project, events per including scientific conferences, and year industrial technology venues	5 per year	35

Standardization contributions	Number of contributions to standardization fora	6	42
Open-source contributions	Number of contributions to open-source initiatives	3	3+
Policy strategies contributions	Number of policies contributed with recommendations	>3	--

Table 3: HORSE's communication KPIs

4.2 Impact Creation Deliverables and Milestones

Table 4 below shows the previous and current impact creation deliverables submitted during the project.

Number	Name	Lead partner	Dissemination level	Due Date	Status at M18
D6.1	Impact Creation Strategy and Plan	MARTEL	PU	M05	Submitted
D6.2	Impact creation report and exploitation strategy	MARTEL	PU	M18	Submitted
D6.3	Final impact creation report and exploitation plan	8BELLS	PU	M36	Current document

Table 4: HORSE impact creation deliverables and milestones

5 IPR Management in the second period of the project (IT2)

Intellectual Property Rights (IPR) management is a critical success factor for maximising the impact, sustainability, and long-term value of research and innovation outcomes, particularly in large-scale collaborative projects like HORSE.

During IT2, the consortium reviewed, updated and finalised the project's intellectual property portfolio, clearly distinguishing between Background and Foreground IP. According to the Article 16.1 of the GA, "Background" (BG) means any data, know-how or information — whatever its form or nature (tangible or intangible), including any rights such as intellectual property rights — that is held by the beneficiaries before they acceded to the Agreement and needed to implement the action or exploit the results. Foreground (FG) refers to the outcomes generated during the project's implementation, encompassing various forms of information, materials, and knowledge. These outcomes represent tangible or intangible outputs resulting from project actions, which may or may not be protectable [1].

Beyond the identification and classification of BG and FG assets, this chapter places strong emphasis on the definition of HORSE Innovations, as well as Exploitable Results (ERs) and Key Exploitable Results (KERs). The selection of the results was based on a set of qualitative and quantitative criteria, including technological maturity, partner interest, and exploitation potential in research, industrial, and market-driven contexts. In parallel, appropriate protection mechanisms and licensing schemes were assessed and documented for each result.

In brief, type of IP protection refers to the specific legal mechanisms used to safeguard intellectual property rights (e.g. copyright, trade secret, proprietary data, patent, trademark etc.). On the other hand, licensing is a legal arrangement in which the owner of intellectual property (the licensor) grants permission to another party (the licensee) to use, produce, or commercialise the intellectual property under defined terms and conditions. (e.g. open source, commercial license, proprietary license etc.) [2]. Regarding the IPR mechanisms of the project's results, it is worth to note that each partner declared the IPR mechanisms that foresee to apply for their results in the future.

Special attention is also given to issues related to joint ownership, which naturally arise in highly collaborative and interdisciplinary projects like HORSE. This chapter outlines the framework used to assess partner contributions to jointly developed results and establishes the basis for the future formulation of Joint Ownership Agreements (JOAs).

Overall, this chapter provides a comprehensive overview of the HORSE IPR management approach, serving as a baseline for the exploitation activities described in the subsequent chapter.

5.1 Background IP

The main BG IPs to be used so as to achieve the objectives of HORSE, as identified and validated by the consortium at the final stage of the project are presented in Table 5. More specifically, the BG table provides an overview of the technological and knowledge assets that pre-existed the start of the project and were utilised within the HORSE framework. Each entry is assigned a unique reference number and includes the official title of the Background asset, the owning partner, and a dedicated internal identifier related to the WP that the BG utilised. Then, a technical description outlines the asset's functionality and relevance to the project objectives, while the corresponding Technology Readiness Level at project start and end indicates its maturity evolution. The table further specifies the foreseen intellectual property protection mechanism (the formal registration will be conducted by each BG owner after the project completion) and the applicable licensing model. In addition, it describes how each BG asset was utilised within the project activities, together with the conditions that governed its use during the project lifetime and beyond its completion. Finally, the table outlines the planned post-project exploitation of each Background technology, including further research, commercialisation, or integration into future products and services.

#	BG Title	Owner	BG Number	Short Description of BG	TRL M1 → TRL M36	Type of IP protection (foreseen)	Licensing	How was it utilised within Project?	Conditions to Use within the Project	Conditions to use outside the Project	How this BG technology will be further exploited after HORSE
1	**Data Fusion Framework (DFF)**	8BELLS	BG4.1	The Data Format Fusion (DFF) aims to bring data-level interoperability and analytics between heterogeneous IoT devices and other functional data pipelines. It is designed based on open-source standards and tools.	3 → 5	Copyright	Proprietary license	As a data distribution platform	Free to use within the project	Subject of licensing agreement	Future commercial launch – will be offered as a subscription service
2	**Comnetsemu network emulator**	CNIT	BG4.2	Network Emulation environment, designed to emulate SDN, NFV and 5G networks.	2 → 4	Copyright	Open source under MIT license	As environment for the SAN and P&P NDT	Free to use within the project	Free to use	Further research

3	**Intent-based Resilience Orchestrator (IRO)**	TUBS	BG5.1	A developed Intent-based resilience orchestration tool which uses Reinforcement Learning for Quality-of-Service assurance.	3 → 6	Copyright	Open source under MIT license	As know-how and as framework for the IBI module	Free to use within the project	Free to use	Further research
4	**Network Function Virtualisation Convergence Layer (NFVCL)**	CNIT	BG5.2	The NFVCL is a network-oriented meta-orchestrator, specifically designed for zeroOps and continuous automation. It can create, deploy and manage the lifecycle of different network ecosystems by consistently coordinating multiple artefacts at any programmability levels (from physical devices to cloud-native microservices).	2 → 4	Copyright	Open source under GPL v3 license	For the CNIT testbed management and deployment of different HORSE components	Free to use within the project	Free to use considering the rules of GPL	Further research
5	**MetalCL**	CNIT	BG5.3	MetalCL is CNIT's automation tool that deploys Network Computing Ecosystems for research by managing bare-metal servers, operating systems, and network devices. It uses virtualization to quickly create, reset, and share complex testing environments, supporting federated testbeds.	2 → 4	Copyright	Open source under GPL v3 license	For the CNIT testbed management and deployment of different HORSE components	Free to use within the project	Free to use considering the rules of GPL	Further research
6	**SPACE (Augmented Reality Engineering Space -AR3S)**	HOLO	BG5.4	An application to visualize and interact with 3D CAD data via Smart Glasses.	4 → 7	Copyright	Commercial license	Support in DEMO#10	Permission from HOLO needed before use	Subject of licensing agreement	Future commercial launch, further research
7	**STREAM (Interactive Streaming for Augmented Reality - ISAR)**	HOLO	BG5.5	STREAM is a software development kit enabling remote application rendering.	6 → 8	Copyright	Commercial license	Support in DEMO#10	Permission from HOLO needed before use	Subject of licensing agreement	Future commercial launch, further research

8	**EFARAIL application**	EFACEC	BG5.6	Application to control vehicle localization and Public Information System in tramway networks.	5 → 6	Trademark	Commercial license	Support in DEMO#9.	Permission from EFACEC needed before use	Subject of licensing agreement	Further research, know-how in future EU projects
9	**Vehicle Simulator**	EFACEC	BG5.7	Simulator of vehicle movement to supply data to EFARAIL application	5 → 6	Trademark	Proprietary license	Used for data tests for EFARAIL application.	Permission from EFACEC needed before use	Subject of licensing agreement	Internal use, further research
10	**PID Simulator**	EFACEC	BG5.8	Simulator for public information display	5 → 6	Trademark	Proprietary license	Used for data tests for EFARAIL application.	Permission from EFACEC needed before use	Subject of licensing agreement	Internal use, further research
11	**BASTION**	UMU	BG5.9	Security orchestrator for applying mitigations in NDTs and UMU testbed.	5 → 6	Copyright	Proprietary license	For UMU testbed and IA-NDT policy management/ enforcement over devices/ nodes	Permission from UMU needed before use	Subject of licensing agreement	Further research

Table 5: HORSE's BG IP

5.2 Foreground IP

Based on the final results of the project that occurred in the completion of the implementation phase, the project partners were given the opportunity to update and finalise the FG IP. The FG table provides an overview of the technologies, components, and knowledge that were generated during the implementation of the HORSE project. Each entry is linked to the relevant work package and identifies the partners that contributed to the development of the result, clearly distinguishing between main and additional contributors. Moreover, each FG asset is associated with a unique internal identifier and is accompanied by a concise technical description outlining its scope, functionality, and relevance to the overall project objectives as well as the activities through which it was developed and validated. The technological maturity of each result is captured through the evolution of its TRL from the beginning to the end of the project, while any dependencies on pre-existing assets are explicitly indicated. The table further documents the foreseen intellectual property protection mechanisms (not formally registered) and licensing models defined by the consortium. It also reports the conditions that governed the use of each FG result during the project lifetime, as well as the conditions applicable after the completion of the project. Finally, it outlines the envisaged post-project evolution of each FG technology, including further research activities and potential commercial exploitation. The updated content is presented in Table 6.

WP	FG Title	Main Contributing Partner	Further Contributing Partner(s)	FG Number	Short Description of FG	Related Tasks and Deliverables	TRL M01 → TRL M036	Related BG (if any)	Type of IP protection (foreseen)	Licensing	Conditions to Use within The Project	Conditions to Use after the end of the Project	How will this FG technology be further exploited and/or developed after the completion of HORSE project
WP3	Predictive Engine and Mitigation (PEM)	ETI	NKUA, 8BELLS (Integration) CNIT (Validation)	FG3.1	Predictive threat detector and mitigation driver for the analysis and processing of network streams in complex network and infrastructure scenarios.	T3.5, All WP3 deliverables	2 → 4	-	Proprietary data	Proprietary license	Free to use	Licence fee based on partners agreement	Internal use, possible future commercial launch integrated in other ETI products

	Network Digital Twin (NDT)	CNIT/TID	UMU (Development support), TUBS (Integration)	FG3.2	Network Digital Twin environment for prediction, prevention and what-if analysis	T3.1, All WP3 deliverables	2 → 4	BG4.2, BG5.9	Copyright	Open source under MIT licence	Free to use	Free to use	Further research
	Distributed Trustable AI Engine (DTE)	NKUA	TUBS, ZORTE (Integration) MAR (Development support)	FG3.3	Distributed threat mitigation environment for the generation of either predictive or corrective intents	T3.3, All WP3 deliverables	2 → 4	-	Copyright	Open source	Free to use	Free to use	Further research
	Early Modelling (EM)	UPC	CNIT, UMU, TID, STS, ETI (Integration and Validation)	FG3.4	Framework for the modelling of vulnerabilities, threats, attacks, proactive actions, mitigations, and estimated impacts.	T3.2, All WP3 deliverables	2 → 4	-	Copyright	Open source	Free to use	Free to use under restrictions	Further research
	Policies and Data Governance (PAG)	SUITE5	-	FG3.5	A module which encrypts and anonymises the collected datasets, and logs the operations performed on the datasets of interest.	T3.4, All WP3 deliverables	2 → 5	-	Copyright	Creative Commons License CC BY-NC	Free to use within the project	License fee based on multi-party exploitation agreements between Suite5 and the party/ies involved in exploitation of results	Upgrade of Suite5 services portfolio of data-driven intelligence with 5G/6G specific technological and innovation know-how, Extend functionality in further research
	Policy Translator (PT)	UMU	TID (Integration) TUBS, UPC (Validation)	FG3.6	Translator between IBI, EM and UMU orchestrator (Bastion) to	T3.1, All WP3 deliverables	2 → 4	BG5.9	Copyright	Open source	Free to use	Free to use	Further research

					execute intents on IA-NDT pods. Allows actions (QoS, Filtering) to be applied and/or metrics queries (monitor) to be performed.								
WP4	Secure e2e Connectivity Manager	CNIT	8BELLS (Integration)	FG4.1	The Secure e2e Connectivity Manager is a key component within the HORSE security infrastructure, which is a state-of-the-art framework developed to protect complex, distributed, and heterogeneous systems.Within this sophisticated ecosystem, the Connectivity Manager functions as a core architectural element, coordinating security-related operations and ensuring comprehensive visibility and control over the various components that form the end-to-end services protected under the HORSE security framework.	T4.2, All WP4 deliverables	2 → 4	BG5.2, BG5.3	Copyright	Open source under GPL v3 license	Free to use	Free to use considering the rules of GPL	Further research

	Reliability Trustworthiness Resilience (RTR)	8BELLS	CNIT, TUBS, MAR (Integration)	FG4.2	Generation of Ansible playbooks via a mitigation action, in order to defend against threats.	T4.1, All WP4 deliverables	2 → 4	-	Copyright	Proprietary license	Free to use	Licence fee based on partners agreement	Future commercial launch – will be offered as a subscription service
	Domain Orchestrator Connector (DOC)	8BELLS	UPC, UMU, CNIT (Integration)	FG4.3	Includes a set of tools to logically and physically interact with the infrastructure elements to provide a secure cross-domain orchestration.	T4.4, All WP4 deliverables	2 → 4	-	Copyright	Proprietary license	Free to use	Licence fee based on partners agreement	Future commercial launch – will be offered as a subscription service
	Pre - processing	8BELLS	STS, ETI, CNIT (Integration)	FG4.4	8BELLS presents a middleware solution designed to orchestrate and bolster a wide array of data sources, ranging in scale and structure, within cohesive and scalable data environments.	T4.3, All WP4 deliverables	2 → 4	BG4.1	Copyright	Proprietary license	Free to use	Licence fee based on partners agreement	Future commercial launch – will be offered as a subscription service
	Compliance Assessment (CAS)	STS	TUBS (Integration)	FG4.5	Sphynx developed a component so HORSE can make sure that every mitigation action that will take place will be compliant to regulations. It also provides an interface for users to check the history of the assessments that	T4.3, All WP4 deliverables	1 → 3	-	Copyright	Proprietary license	Free to use	Free to use	Further research, Future commercial launch inside the core STS platform

					took place and their result								
	Smart Monitoring (SM)	STS	CNIT, UPC (Integration) 8BELLS, ZORTE (Validation)	FG4.6	Responsible for the collection, transformation and digestion of data from all various and diverse domain resources, as well as data related to the usage of the resources involved in the lifecycle management.	T4.3, All WP4 deliverables	2 → 4	-	Copyright	Proprietary license	Free to use	Free to use	Further research, Future commercial launch
	Common Knowledge Base (CKB)	MAR	TUBS, UPC (Integration)	FG4.7	The CKB is an intelligent system that harnesses the power of multiple state-of-the-art LLMs to dynamically enrich a cybersecurity knowledge base, going beyond traditional static knowledge bases.	T4.1, D4.2	2 → 4	BG4.3	Copyright	Open source under GNU General Public License v3.0	Free to use	Free to use	Further research, possible future commercial launch integrated in other MAR products
WP5	Intent-based Interface (IBI)	TUBS	8BELLS, TID, STS, ZORTE (Integration and Validation)	FG5.1	The HORSE Intent-Based Interface is responsible for mapping high-level intents from a user, received as structured text or through a dedicated API, and further mapping those intents into use requirements. The requirements are then used to	T5.1, D5.2, D5.3	2 → 4	BG5.1	Copyright	Open source under MIT license	Free to use	Free to use	Further research

					propose a list of deployable network policies that can mitigate attacks happening in the network or prevent future attacks. The policies are sent to a lower-level controller for deployment and enforcement in the network elements.								

Table 6: HORSE's FG IP

5.3 HORSE Innovations

Considering HORSE's BG and FG, the project partners were given the opportunity to update the Innovations Matrix based on the overall progress achieved during the final stage of the implementation phase. The updated content is presented in Table 7.

Innovation ID	Key Innovation To research	Lead Partner	TRL M01 → TRL M036	Rationale (Means of Verification)
I01	Intent-based management interface	TUBS	2 → 4	An Intent management interface to automate the processing and deployment of the user intents and their interactions with other modules (D5.2, D5.3).
I02	Attacks characterization and modelling	UPC	2 → 4	Definition of a complete taxonomy of attacks models, to quantify the potential impact on the system (D3.1, D3.2).
I03	Network Digital Twin environment	TID / CNIT	2 → 4	Availability of a network Digital Twin environment able to support the verification of end-to-end network scenarios, with specific focus on security (D3.1, D3.2).
I04	Threat Detection and Mitigation	ETI	2 → 4	Innovation point: Among the different ML algorithms, a novel algorithm conceived in the Ericsson Labs and patent protected will be implemented and tested for the first time. Its performances will be compared with the current benchmarks. The detector internal architecture is innovatively presenting a multistage ML system where every stage learns from the outcomes of the previous one. This innovative scheme will allow many competitive benefits: a) A higher automation level (auto

				calculation of all the thresholds) b) A better visibility, that mean more effectiveness for combined or zero-day new forms of attacks. At Horse framework level: The innovative combination of a Machine Learning threat detector And of a Digital Twin will innovatively allow a more effective mitigation strategy precisely dynamically modulating the required actions minimizing the network impairments.
I05	End-to-end secure connectivity manager	CNIT	2 → 4	Availability of an end-to-end secure connectivity manager, an OSS module based on OSM, capable of orchestrating the requests by PIL to the available infrastructure domain (D4.1, D4.2).
I06	Security for Advanced Communication Techniques	NKUA	2 → 4	Investigation of PLS aspects related to the evolving 6G technologies, considering the energy efficiency and the signalling overhead (D3.1, D3.2).
I07	Distributed Trustable AI Engine	NKUA	2 → 4	The target is to develop distributed AI solutions to secure the 6G network from unknown attacks (D3.1, D3.2).
I08	Security & Privacy Assurance Platform	STS	4 → 6	The security assurance platform combines runtime monitoring, dynamic and static testing, and impact assessments to provide a real-time security posture assessment and certification of

				heterogeneous systems (D4.1, D4.2).
I09	Data Fusion Mechanism	8BELLS	3 → 5	With regards to Smart Monitoring, 8BELLS offers a middleware solution in order to be able to orchestrate and support large scale and structurally different data sources under common and expandable data spaces. The above-mentioned mechanism greatly enhances data interoperability, through the adoption of common APIs for data exchange, and the definition of common data models. APIs for data and metadata management, as well as standardized endpoints for sophisticated queries are supported (D3.2, D4.2).

Table 7: HORSE's Innovations

5.4 Exploitable results and ownership proposition

The methodology adopted in the HORSE project for deriving Exploitable Results (ERs) is based on FG technologies or, in specific cases, on the combination of BG and FG technologies presented in the previous subchapters, with the highest exploitation potential. The main results of HORSE, as identified, updated, and validated by the consortium at the final stage of the project, along with their description and the corresponding ER number, are presented in Table 8.

ER number	ER Title	Main Partner(s)	Further Contributing Partners	Short Description of ER	Related Tasks and Deliverables	TRL M01 → TRL M036	Related BG number (if any)	Related FG number(s)	Proposition of ER Owner	Type of IP protection (foreseen)	Licensing
ER1	Reliability Trustworthiness Resilience (RTR)	8BELLS	TUBS MAR, CNIT (Integration)	Generation of Ansible playbooks via a mitigation action, in order to defend against threats.	T4.2, All WP4 deliverables	2 à 4	-	FG4.2	8BELLS	Copyright	Proprietary license
ER2	Early Modelling (EM)	UPC	CNIT, UMU, TID, STS, ETI (Integration and Validation)	Framework for the modelling of vulnerabilities, threats, attacks, proactive actions, mitigations, and estimated impacts.	T3.2, All WP3 deliverables	2 → 4	-	FG3.4	UPC	Copyright	Open source
ER3	Intent-Based Interface (IBI)	TUBS	8BELLS, NKUA, TID, STS (Integration and Validation)	A collection of tools that proposes low-level network policies in response to security threats and vulnerabilities detected in the network based in high-level user's intents related to resiliency, quality of service, and availability.	T5.1, D5.2, D5.3	2 → 4	BG5.1	FG5.1	TUBS	Copyright	Open source under MIT license

ER4	Policies and Data Governance (PAG)	SUITE5	-	Experiment on and implement new encryption, anonymisation and data observability techniques. Upgrade of Suite5 services portfolio of data-driven intelligence with 5G/6G specific technological and innovation know-how.	T3.4, All WP3 deliverables	2 → 5	-	FG3.5	SUITE5	Copyright	Creative Commons License CC BY-NC
ER5	Pre-Processing	8BELLS	STS, ETI, CNIT (Integration)	8BELLS presents a middleware solution designed to orchestrate and bolster a wide array of data sources, ranging in scale and structure, within cohesive and scalable data environments.	T4.3, All WP4 deliverables	2 → 4	BG 4.1	FG3.6	8BELLS	Copyright	Proprietary license
ER6	HORSE Platform	CNIT/UPC	ALL (Development support and Integration)	Complete set of features and functionalities towards a secure 6G system orchestration.	All Tasks and deliverables of WP2	2 → 5	ALL	ALL	CNIT/UPC	To be discussed in the future	Open source under Apache 2.0 license

ER7	Distributed AI Engine for Services Preassessment	NKUA	MAR, ZORTE, UPC, TUBS, CNIT (Development support) STS, 8BELLS, S5, TID (Integration)	Set of functionalities (Sandboxing, AI contextual models, etc.) to be used to replicate the entire 6G landscape in order to conduct a preliminary performance assessment of the tentative orchestration strategies to be deployed, aimed at ensuring that all deployed services run in a secure, distributed and optimized environment.	T3.3, All WP3 deliverables	2 → 4	BG5.1	FG3.3, FG5.1	NKUA	Copyright	Open source under Apache 2.0 license
ER8	Smart Monitoring (SM)	STS	CNIT, UPC (Integration) 8BELLS, ZORTE (Validation)	Responsible for the collection of data from all various and diverse domain resources, as well as data related to the usage of the resources involved in the lifecycle management.	T4.3, All WP4 Deliverables	2 → 4	-	FG4.6	STS	Copyright	Open source under Apache 2.0 license
ER9	Threat detection and Mitigation Engine (DEME)	ETI	NKUA, 8BELLS (Integration) CNIT (Validation)	Tool responsible for detecting threats in a predictive form, thus proactively acting towards removing or in the worst case mitigating the impact of the foreseen threat.	T3.5, All WP3 deliverables	2 → 4	-	FG3.1	ETI	Proprietary data	Ericsson proprietary license
ER10	Intent-based Secure cross – Domain Orchestrator	8BELLS	CNIT, TUBS, MAR, UPC, UMU (Integration)	Includes a set of tools to logically and physically interact with the infrastructure elements to provide a secure cross-domain orchestration. The interaction will be handled through a	T4.1, T4.4, All WP4 deliverables	3 → 5	-	FG4.2, FG4.3, FG5.1	8BELLS	Copyright	Proprietary license

				proper mapping of high-level intents into security workflows able to react to security threats and vulnerabilities.							
ER11	End to end Proactive Secure Connectivity Manager (ePEM)	CNIT	8BELLS (Integration)	ePEM plays a pivotal role in the HORSE security infrastructure. HORSE represents a cutting-edge security infrastructure designed to safeguard complex, distributed, and heterogeneous systems. In this intricate environment, the ePEM serves as a central architectural element, orchestrating actions and providing observability over the various components that constitute the end-to-end services secured within the HORSE security perimeter.	T4.2, All WP4 deliverables	2 → 4	BG5.2, BG5.3	FG4.1	CNIT	Copyright	Open source under GPL v3 license
ER12	Network Digital Twin (NDT)	TID/CNIT	UMU (Development support), TUBS (Integration)	An environment for testing "what-if" scenarios and performing predictions on the state of the network. The Network Digital Twin represents an isolated environment which accurately replicates the original 6G network as well as services and traffic.	T3.1, All WP3 deliverables	2 → 4	BG4.2, BG5.9	FG3.2	TID/CNIT	Copyright	Open source under MIT licence

Table 8: HORSE's ERs

5.5 Key Exploitable Results and ownership proposition

Projects with the scale of impact, ambition and multidisciplinary collaboration as HORSE naturally generate a wide range of ERs. However, some of these results may appeal only to specific partners or may require further development before becoming suitable for commercial, internal, or scientific exploitation. To ensure effective post-project utilisation and to maximise overall impact, it is essential to focus the exploitation strategy on those results with the highest potential for exploitation, impact and added value identified as Key Exploitable Results (KERs).

Following a thorough evaluation of each ER listed in Table 8, considering technical maturity, partner interest and post-project exploitation potential, the consortium identified the HORSE KERs presented in Table 9.

ER number	ER Title	Main Partner(s)	Further Contributing Partners	Short Description of ER	Related Tasks and Deliverables	TRL M01 → TRL M036	Related BG number (if any)	Related FG number(s)	Proposition of ER Owner	Type of IP protection (foreseen)	Licensing
KER1	HORSE Platform	CNIT/UPC	ALL (Development support and Integration)	Complete set of features and functionalities towards a secure 6G system orchestration.	All Tasks and deliverables of WP2	2 → 5	ALL	ALL	CNIT/UPC	To be discussed in the future	Open source under Apache 2.0 license
KER2	Distributed AI Engine for Services Preassessment	NKUA	MAR, ZORTE, UPC, TUBS, CNIT (Development support) STS, 8BELLS, S5, TID (Integration)	Set of functionalities (Sandboxing, AI contextual models, etc.) to be used to replicate the entire 6G landscape in order to conduct a preliminary performance assessment of the tentative orchestration strategies to be deployed, aimed at ensuring that all deployed services run in a secure, distributed and optimized environment.	T3.3, All WP3 deliverables	2 → 4	BG5.1	FG3.3, FG5.1	NKUA	Copyright	Open source under Apache 2.0 license

KER3	Smart Monitoring (SM)	STS	CNIT, UPC (Integration) 8BELLS, ZORTE (Validation)	Responsible for the collection of data from all various and diverse domain resources, as well as data related to the usage of the resources involved in the lifecycle management.	T4.3, All WP4 Deliverables	2 → 4	-	FG4.6	STS	Copyright	Open source under Apache 2.0 license
KER4	Threat detection and Mitigation Engine (DEME)	ETI	NKUA, 8BELLS (Integration) CNIT (Validation)	Tool responsible for detecting threats in a predictive form, thus proactively acting towards removing or in the worst case mitigating the impact of the foreseen threat.	T3.5, All WP3 deliverables	2 → 4	-	FG3.1	ETI	Proprietary data	Ericsson proprietary license
KER5	Intent-based Secure cross – Domain Orchestrator	8BELLS	CNIT, TUBS, MAR, UPC, UMU (Integration)	Includes a set of tools to logically and physically interact with the infrastructure elements to provide a secure cross-domain orchestration. The interaction will be handled through a proper mapping of high-level intents into security workflows able to react to security threats and vulnerabilities.	T4.1, T4.4, All WP4 deliverables	3 → 5	-	FG4.2, FG4.3, FG5.1	8BELLS	Copyright	Proprietary license
KER6	End to end Proactive Secure Connectivity Manager (ePEM)	CNIT	8BELLS (Integration)	ePEM plays a pivotal role in the HORSE security infrastructure. HORSE represents a cutting-edge security infrastructure designed to safeguard complex, distributed, and heterogeneous systems. In this intricate environment, the ePEM serves as a central architectural element, orchestrating actions and providing observability over the various components that	T4.2, All WP4 deliverables	2 → 4	BG5.2, BG5.3	FG4.1	CNIT	Copyright	Open source under GPL v3 license

				constitute the end-to-end services secured within the HORSE security perimeter.							
KER7	Network Digital Twin (NDT)	TID/CNIT	UMU (Development support), TUBS (Integration)	An environment for testing "what-if" scenarios and performing predictions on the state of the network. The Network Digital Twin represents an isolated environment which accurately replicates the original 6G network as well as services and traffic.	T3.1, All WP3 deliverables	2 → 4	BG4.2, BG5.9	FG3.2	TID/CNIT	Copyright	Open source under MIT licence

Table 9: HORSE's KERs

5.6 Joint Ownership Agreement (JOA): terms of exercise per HORSE Key Exploitable Result

As per subchapter of Article 16 “Ownership of results” of the HORSE GA, two or more partners can exploit their own results jointly in the cases that they have generated them jointly. Partners can jointly exploit results via a written agreement, to ensure compliance with their obligations under this Agreement.

More specifically, joint ownership of results is established when:

- they are co-created by two or more project beneficiaries
- it is not possible to:
    - determine the individual contributions of each beneficiary
    - separate the contributions for the purposes of applying for, obtaining, or maintaining protection

Joint owners must reach a consensus (documented in writing) regarding the division and conditions of their joint ownership (referred to as the “Joint Ownership Agreement”), to adhere to their commitments under this Agreement.

To ensure a fair and transparent definition of the ownership structure for each KER, dedicated discussions were held among the consortium partners. Each partner’s contribution was assessed based on its level of involvement in the development of KER, as reflected in Table 9. Accordingly, the Main Partners are those who provided the major or full contribution to the creation of the respective KERs. Partners who were involved mainly through minor development support, integration and/or validation activities were considered as Further Contributing Partners and therefore do not hold ownership percentages.

Following this, a series of bilateral and multilateral discussions with the consortium partners were held to calculate and assign the contribution percentages for each KER. Table 10 details the quantitative contributions of each beneficiary towards the HORSE project’s KERs.

KER Parties' Contribution (%)															
KER number	Title	CNIT	TID	ETI	TUBS	NKUA	S5	UPC	EFACEC	HOLO	ZORTE	8BELLS	MAR	STS	UMU
KER1	HORSE Platform	11%	6.5%	6.5%	6.5%	6.5%	6.5%	11%	6.5%	6.5%	6.5%	6.5%	6.5%	6.5%	6.5%
KER2	Distributed AI Engine for Services Preassessment					100%									
KER3	Smart Monitoring (SM)													100%	
KER4	Threat detection and Mitigation Engine (DEME)			100%											

KER5	Intent-based Secure cross – Domain Orchestrator											100%			
KER6	End to end Proactive Secure Connectivity Manager (ePEM)	100%													
KER7	Network Digital Twin (NDT)	50%	50%												

Table 10:Quantitative contributions per KER

In the case of KER1 (HORSE Platform), the consortium agreed that all partners should hold a share of ownership in order to reflect the integration of multiple technological contributions from each of them. Given their key roles in the project coordination and overall technical management, CNIT (Project Coordinator) and UPC (Technical Coordinator) were assigned a slightly higher ownership percentage to acknowledge their overarching responsibilities in leading, integrating, and maintaining the platform architecture. All other partners share equal ownership percentages and will be considered as Main partners in this KER.

The insights from the above table serve as the essential basis for forming Joint Ownership Agreements (JOAs) between the Main Partners of each KER. These agreements aim to govern the use of KERs after the project ends. They may be structured as either bilateral contracts (between two partners) or multilateral contracts (involving multiple partners). All parties involved have concurred that the execution of the JOAs should be deferred until after the end of the project timeline for several key reasons:

- **Technology Readiness Level (TRL) of the KERs:** The KERs mentioned are currently at an early stage of development, with a TRL not high enough for widespread market use. All HORSE KERs have reached only up to TRL 5, indicating that they are still undergoing laboratory testing and validation in a relevant environment to finalise any JOA, it is necessary to advance these technologies to higher TRLs to ensure they meet required standards for deployment and market entry.

- **Further Development and Testing Needed:** Beyond TRL considerations, the KERs require further development and thorough testing to confirm they meet all commercial performance and safety standards. Committing prematurely to JOA could result in unforeseen challenges and obligations, as incomplete validation might lead to issues in real-world deployment, regulatory compliance, or market acceptance.

- **Compliance with Legal and Regulatory Standards:** Drafting and finalising such agreements necessitate adherence to a complex web of legal and regulatory frameworks at national, European, and international levels, including trade regulations, IP rights, and export controls. This compliance process is intricate, demanding meticulous attention and expert legal counsel for all signatory entities.

- **Contractual Complexity:** The nature of JOAs demands engagement from senior-level officials from each participating organisation, which involves aligning various interests and negotiating the legal terms, a process that is inherently detailed and prolonged. Such coordination and agreement finalization could not feasibly occur within the project's timeframe, especially prior to finalizing the content of this document.

- **Market Feasibility Analysis:** The decision to sign a JOA also depends on each partner conducting detailed market feasibility analyses for the exploitable results of interest. These studies are vital to assess market potential, identify risks, and develop a solid commercialisation plan after the project ends. Although support from services like the Booster is partially available during the project, this responsibility generally lies with the specialised departments within each organisation. Market feasibility analysis is a complex task often extending beyond the project timeline and requires sufficient time to ensure thoroughness and relevance, allowing completion well after project closure.

Until the formal execution of the JOAs, each co-owner shall be required to obtain the prior written consent of all other co-owners before engaging in any commercial or developmental activity involving the jointly owned KERs such as any sale, licensing, transfer, or further development with third parties.

6 Exploitation Activities

The exploitation of project results is a cornerstone of the HORSE impact strategy and a key element in ensuring that the project's outcomes generate sustainable value beyond its lifetime.

Given the heterogeneous nature of the HORSE consortium (bringing together research organisations, universities, large industrial players and SMEs) exploitation is not limited to purely commercial pathways. Instead, a multidimensional approach is adopted, encompassing commercial, internal, research, and other exploitation types, thereby allowing each partner to leverage the project results in line with its strategic objectives, capabilities, and long-term vision.

Within this context, the chapter initially introduces the main categories of exploitation routes, aligned with the overall HORSE IPR strategy. It then details the exploitation types and pathways per partner and per ER, clearly distinguishing between the nature of exploitation (how the results are used) and the concrete pathways through which results may reach markets, end users, research communities, or policy and standardisation bodies.

Particular emphasis is placed on the KERs, which concentrate the highest potential for impact and sustainability. The KERs formed the core focus of the project's targeted exploitation efforts and were further developed through the participation of HORSE in the Horizon Results Booster (HRB) programme, specifically within the Go-to-Market (G2M) service.

Furthermore, the chapter presents the individual exploitation plan for each party as well as the contribution of HORSE to European and global sustainability objectives, including the UN Sustainable Development Goals.

6.1 Potential exploitation types

Understanding partners' exploitation interest is essential to identify their expectations regarding the use of each ER they helped develop. Since the consortium includes partners with diverse orientations, such as research institutions, industries, and universities, it is natural that their individual exploitation interests for each result will vary. The main exploitation routes commonly used in Horizon R&D projects, now adapted to the HORSE IPR strategy, are summarised in the following chapters:

Commercial

The commercial exploitation avenues identified below aim to utilise the project's outcomes with a commercial objective: to increase profits and/or market competitiveness for the partners involved. More specifically, those exploitation avenues may be:

- Offer HORSE's human-centric, open-source and sustainable platform solutions to telecommunications providers for enhancing 6G network operations, orchestration, and security.
- Deploy HORSE technologies in Industry 4.0 environments enabling multi-user XR collaboration, secure infrastructure management, and real-time adaptive network provisioning.
- Provide consultancy and integration services to customize and deploy HORSE's evolutionary coordination and protection platform within enterprise cloud and edge environments.
- Partner with network operators, and vertical sector stakeholders to create joint ventures exploiting HORSE solutions across 6G-related fields.

Internal

The “Internal” exploitation type refers to using project outcomes to enhance an organisation's internal processes or products. HORSE partners may anticipate utilising the results as follows:

- Enhance internal processes/products related to 5G/6G security for performance improvement.
- Incorporate HORSE outcomes to expand their portfolio and refine existing products.
- Leverage HORSE outcomes to boost knowledge, conduct further research, and explore new opportunities.

Research

The "Research" exploitation type involves using project results for scientific purposes, potentially leading to new research projects, publications, or novel research concepts, without immediate commercialisation intent. HORSE partners may envisage the following research exploitation paths:

- Utilise HORSE results for ongoing and future research projects, particularly by academic researchers and research centers.
- Advance research collaborations between industry, academia, and government in 5G/6G security topics.

Other

The "Other" category encompasses exploitation types not covered under commercial, research, or internal categories, potentially including civic, humanitarian, or policy-related purposes, such as making HORSE results available to open-source communities or enhancing the overall 5G/6G security environment.

6.2 Exploitation types and pathways per HORSE partner

The following tables (Table 11 and Table 12) outlines the varied exploitation interests of each partner regarding the ERs, based on their role as either a lead or contributing entity in the respective project outcomes.

More specifically, exploitation type refers to the category or kind of exploitation of the project results, meaning the way the results are intended to be used. On the other hand, exploitation pathway describes the specific route or process through which the exploitation of the result will be realised. In other words, how the results will reach the market or end users [3].

Partners had the option to categorise their interest in each exploitable asset into one (or more) of four distinct exploitation types (see chapter 4.2 for more details):

(i) C – Commercial,
(ii) I – Internal,
(iii) R – Research,
(iv) O – Other.

Given that the project is nearing completion, the partners’ interests in exploitation have been updated to reflect the latest project advancements.

To adhere to the IPR (co)ownership of the ERs, a partner was eligible to declare a Commercial Exploitation interest only if they were identified as a Main Partner (referenced in Table 8).

In addition, while the declaration of Commercial exploitation is limited to the Main Partners in line with IPR co-ownership, the Contributing Partners were also invited to provide input in this section. Their feedback is essential to capture the broader exploitation perspective of the project results, particularly regarding Internal, Research, or Other exploitation routes.

It should be noted that the indication of exploitation types and pathways by the Contributing Partners, who supported the ERs through development, integration and/or validation activities (as shown in Table 8), does not imply ownership rights over the respective ERs. Such declarations are intended to capture potential interest or intent to explore collaboration, licensing and/or future utilisation opportunities, subject to agreement with the respective Main Partner(s) who hold the IPR. Therefore, if a Contributing Partner wished to express potential interest on an ER, a Potential Exploitation Interest (PEI) tag used to indicate non-binding intentions to explore future use or collaboration opportunities.

Potential Exploitation Types per HORSE partner															
ER number	Title	CNIT	TID	ETI	TUBS	NKUA	S5	UPC	EFACEC	HOLO	ZORTE	8BELLS	MAR	STS	UMU
ER1	Reliability Trustworthiness Resilience (RTR)	I, R (PEI)										I, R			
ER2	Early Modelling (EM)	I, R (PEI)						R							
ER3	Intent-Based Interface (IBI)	I, R (PEI)			I, R	R (PEI)					I, R (PEI)				
ER4	Policies and Data Governance (PAG)						I, R								

ER5	Pre-Processing	I, R (PEI)									I, R				
ER6 / KER1	HORSE Platform	I, R	I, R	I, R	I, R	I, R	R	R	R	R	I, R	I, R	R	R	R
ER7 / KER2	Distributed AI Engine for Services Preassessment					C, R		R (PEI)							
ER8 / KER3	Smart Monitoring (SM)										I, R (PEI)			I, R	
ER9 / KER4	Threat detection and Mitigation Engine (DEME)			I, C											
ER10 / KER5	Intent-based Secure cross – Domain Orchestrator											I, R			

ER11 / KER6	End to end Proactive Secure Connectivity Manager (ePEM)	I, R													
ER12 / KER7	Network Digital Twin	I, R	I, R		I, R (PEI)						I, R (PEI)				

Table 11: Exploitation types per partner for ERs

Moreover, the following table (Table 12) illustrate the exploitation strategies for each partner concerning the ERs respectively, considering whether a partner has led or contributed to the development of the respective outcome. Partners were given the choice of five different pathways for exploiting each result:

(i) M: Creating a product for sale,
(ii) U: Utilising the project results internally to aid further development, such as creating additional products for sale or enabling R&D departments (both public and private) to leverage the findings in new research endeavours
(iii) L: Licensing the project outcome to external parties,
(iv) S: Offering Services like consultancy, training etc.,
(v) A: Academic exploitation, meaning open-source availability and standardisation influence,
(vi) O: Other approaches.

Consistent with the IPR (co)ownership rules for the HORSE ERs, only partners recognised as Main Partners (as per Table 8) were permitted to choose a commercialisation-focused exploitation path for a particular ER (e.g., manufacturing and selling a product, licensing the project outcome). On the other hand, contributing partners were allowed to offer services such as consulting, training or operational support or use the results internally.

Potential Exploitation Pathways per HORSE partner															
ER number	**Title**	**CNIT**	**TID**	**ETI**	**TUBS**	**NKUA**	**S5**	**UPC**	**EFACEC**	**HOLO**	**ZORTE**	**8BELLS**	**MAR**	**STS**	**UMU**
ER1	**Reliability Trustworthiness Resilience (RTR)**	**U**										**U, L, S**			

ER2	Early Modelling (EM)	U						U, S							
ER3	Intent-Based Interface (IBI)	U			U, A	U					U, S				
ER4	Policies and Data Governance (PAG)						U, L								
ER5	Pre-Processing	U										U, L, S			
ER6 / KER1	HORSE Platform	U, S	U, A*	U	U, A	U, S	U	U, S	U, S	U	U, S	U, S	U	U	U
ER7 / KER2	Distributed AI Engine for					U, S, A		U, S							

	Services Preassessment														
ER8 / KER3	Smart Monitoring (SM)										U, S			U	
ER9 / KER4	Threat detection and Mitigation Engine (DEME)			U											
ER10 / KER5	Intent-based Secure cross – Domain Orchestrator											U, L, S			
ER11 / KER6	End to end Proactive Secure Connectivity Manager (ePEM)	U, S, A													
ER12 / KER7	Network Digital Twin	U, S, A	U, A*		U						U, S				

Table 12: Exploitation strategy for ERs per partner

* Mainly focus on standardisation and collaboration with universities

6.3 Horizon Results Booster

The Horizon Results Booster (HRB) [4] is a unique initiative from the European Commission (EC) designed to help research and innovation projects (funded under Horizon Europe, Horizon 2020, and FP7) maximise the impact of their results on society and the market. The HRB offers beneficiaries free-of-charge expert support and tools to facilitate both the dissemination and exploitation of project outcomes. Its objective is to bridge the gap between research and tangible societal benefits by transferring scientific achievements into real-world value and innovation.

As part of the project's Exploitation task, the HORSE consortium, taking into account its needs and the available bundles of service offered by the HRB, applied for 2.3 Go-to-market support (G2M) service in February 2025. The HRB application was successfully accepted on March 2025.

The aim of G2M service is to assist beneficiaries in advancing their KERs toward market readiness. It also supports the development of a business plan and identifies opportunities for further exploitation or reuse of research results. Through coaching, beneficiaries have the opportunity to assess result maturity, conduct market analysis, perform risk assessments, and identify key stakeholders and business partners.

Upon assignment of the experts a couple of entry level meetings held on April 2025. During those meetings, all the KER main partners (Table 9) presented the HORSE project into the experts and received initial consultations which helped select the most suitable strategies for exploitation. The mentors guided the project team through the HRB ecosystem, assessed their existing exploitation plans, and as a result a customised roadmap for the G2M HRB services was designed (Table 13).

Exploitation intentions table for KER…	
Booster services	**Timing**
2.3 Go-to Market-Module A: Kick off	**May 2025**
2.3 Go-to-Market-Module B: Unique Value Proposition and KERs	**June 2025**
2.3 Go-to Market-Module C: Exploitation Strategy	**July 2025**
2.3 Go-to Market-Module D: Business Plan	**September 2025**
2.3 Go-to Market-Module E: Access to other funding & entrepreneurship support	**October 2025**
2.3 Go-to Market-Module F: Reporting	**November 2025**

Table 13: Roadmap of HORSE HRB service

More specifically, the G2M support consisted of six Modules (phases), during which the KER teams (main partners and supporters), with the assistance of the HRB experts, were required to complete specific templates related to each Module. Also, it is worth to note that the G2M service focuses on a maximum of three KERs, which are selected by the HORSE consortium at the end of Module A. Since HORSE has seven KERs in total, the exploitation team decided to use the same templates and follow the same review structure applied by the HRB expert for the remaining four KERs. This ensures that the content provided in this deliverable is consistent across all KERs.

6.3.1 Step-by-step workflow for each Module

Each Module in the HRB followed a structured workflow (Figure 14). The process began with the provision of specialised templates by the experts, which were introduced during dedicated workshops where the experts and KER teams discussed the relevant topics and requirements for each Module.

After the workshop, the KER teams prepared the initial versions of the templates and submitted them to the HRB expert for review. Additional workshops were then organised to discuss, review and refine the templates based on the expert's feedback.

The workflow concluded with the finalisation of the templates and the preparation of detailed documentation by the HRB expert, summarising the work completed in each Module. Once this step was completed, the Module was officially closed.

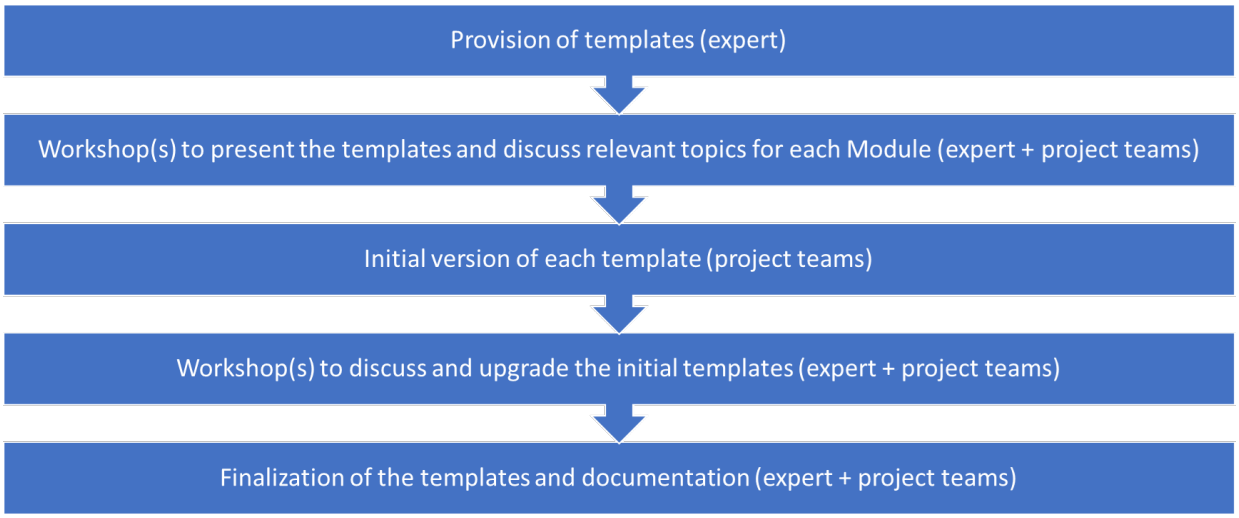


Figure 14: The step-by-step workflow for HRB Modules

The following subchapters present an introduction and the revised templates (either by the HRB expert or by the HORSE exploitation manager) for all KERs for each Module.

6.3.2 Module A: Kick off

The Module A is the starting point of the HRB's G2M support. The main objective of this module is to lay a solid foundation for the upcoming exploitation strategy activities. Another crucial element of Module A is the delivery of targeted training on the exploitation pillars, focusing on the G2M process and related concepts.

During the initial meetings with the Booster expert, the service and tools for all Modules were presented and also, all KER teams were requested to complete the "Exploitation Intentions Table" (Table 14) which was the first (and only) template for Module A.

Exploitation intentions table for KER…	
Description	Description of what the KER is.
Target market/ end users	Describe the market in which the KER will be possibly used/can "compete by".
Competitive advantages	Description of the KER's competitive advantages e.g. how much better does your KER solve the end-users' needs/problems compared to competition? or What distinguishes the KER from the competition/current solutions? etc.
Use model	Description of how the KER will be put into use.
Partners	The consortium partner(s) willing to exploit the KER after the end of the project.
Timing	The time to market.
IP status	The IPR strategy for the KER.

Table 14: The "Exploitation Intentions Table"

More specifically, the "Exploitation Intentions Table" is designed to capture essential information about each KER. Each row represents a different KER, while the columns solicit detailed input from beneficiaries to guide effective exploitation planning. The columns include a description of the KER followed by an analysis of the target market and end users and also identifying who will benefit, the primary audience and the market needs addressed. There's also a section for competitive advantages, where beneficiaries describe what differentiates their KER from existing solutions and how it better solves end-user problems. The use model column requires an explanation of how the KER will be adopted in practice, whether through services, products, licensing, or other means, and identifies potential early adopters. Additional columns list project partners involved in post-project exploitation, the expected timing for market entry and the relevance and strategy for IP management.

The "Exploitation Intentions Tables" in Appendix B – Module A templates correspond to each HORSE KER and have all been reviewed by the HRB expert.

6.3.3 Module B: Unique Value Proposition and KERs

Module B is the second part of the HRB services. Briefly, the objectives of this Module are:

- To evaluate the project's KERs, identify and prioritize the three most impactful ones to be further developed within the HRB framework; define the unique value proposition (UVP) for each selected KER; and analyse their intellectual assets (IA), including the corresponding IA management strategy. Out of the seven KERs produced by the project, KER1, KER5, and KER7 were selected by the consortium for continued

development with the support of the Booster expert, while the remaining KERs were assessed by the project's exploitation manager in alignment with the Booster expert's review.

- To conduct desk research on the project's KERs, covering aspects such as the nature of the results, technology readiness levels, relevant standards, patents, and other pertinent information; and to organize a workshop to discuss the findings, including target markets, customer segments, and potential early adopters.

This module comprises two templates: the UVP Canvas (Table 15) and the Market Definition Canvas (Table 16), both of which are depicted in the following pages.

Briefly, the Value Proposition Canvas is a strategic tool used to ensure a strong alignment between a solution and the specific needs of a targeted customer segment. It is structured around two main components: the Customer Profile and the Value Map. The Customer Profile captures what customers are trying to achieve through their jobs, the pains they experience before, during, or after performing these jobs, and the gains they expect or desire. The Value Map focuses on the solution itself and describes how the proposed products and services address customer needs. It details the offered products and services, explains how they act as pain relievers by reducing or eliminating customer frustrations, and outlines gain creators that deliver tangible or intangible benefits.

On the other hand, the Market Definition Canvas is a structured framework used to clearly define and scope the target market of a product, service, or innovation by focusing on the concept of "jobs to be done." Rather than relying solely on traditional market segmentation, this canvas emphasizes who the users are, what job they are trying to accomplish, and in what context. It begins with a traditional market definition and progressively refines it by identifying the job executors and abstracting them into broader user categories. Central to the canvas is the definition of the Job-to-be-Done, which represents the core problem or task that users aim to solve. The canvas further explores the functional role of the product in helping users accomplish this job, as well as other products or solutions currently used for the same or related purposes.

The development of the UVP and Market Definition Canvases for the KERs aimed to clarify the value each KER delivers and to explicitly link it to concrete market needs and user problems and supported the transition from a purely technology-driven description of the KERs to a user-centric perspective, focusing on the jobs-to-be-done, the pains experienced by target users, and the gains they expect.

In parallel, the Market Definition Canvases were used to precisely define who the users or customers are for each KER, in which context they operate, and which alternative products or solutions they currently rely on.

Briefly, a key horizontal outcome of Module B was the identification of clear and complementary value propositions, even for KERs addressing different technical layers of the HORSE architecture. While individual KERs target distinct functionalities (e.g. monitoring, orchestration, AI-based assessment, mitigation), they consistently demonstrate shared competitive advantages such as automation, scalability, interoperability, and integration within a system-level platform. To sum up, the analysis conducted in Module B can position the HORSE solutions within the 5G/6G value chain, clarifying the roles and different characteristics of each key stakeholder.

Both templates were completed for each KER, reviewed by either the Booster expert or the project's exploitation manager, and are available at the Appendix C – Module B templates.

The Value Proposition Canvas

Customer Segment: *The customer segment that can benefit the most from the KER.*

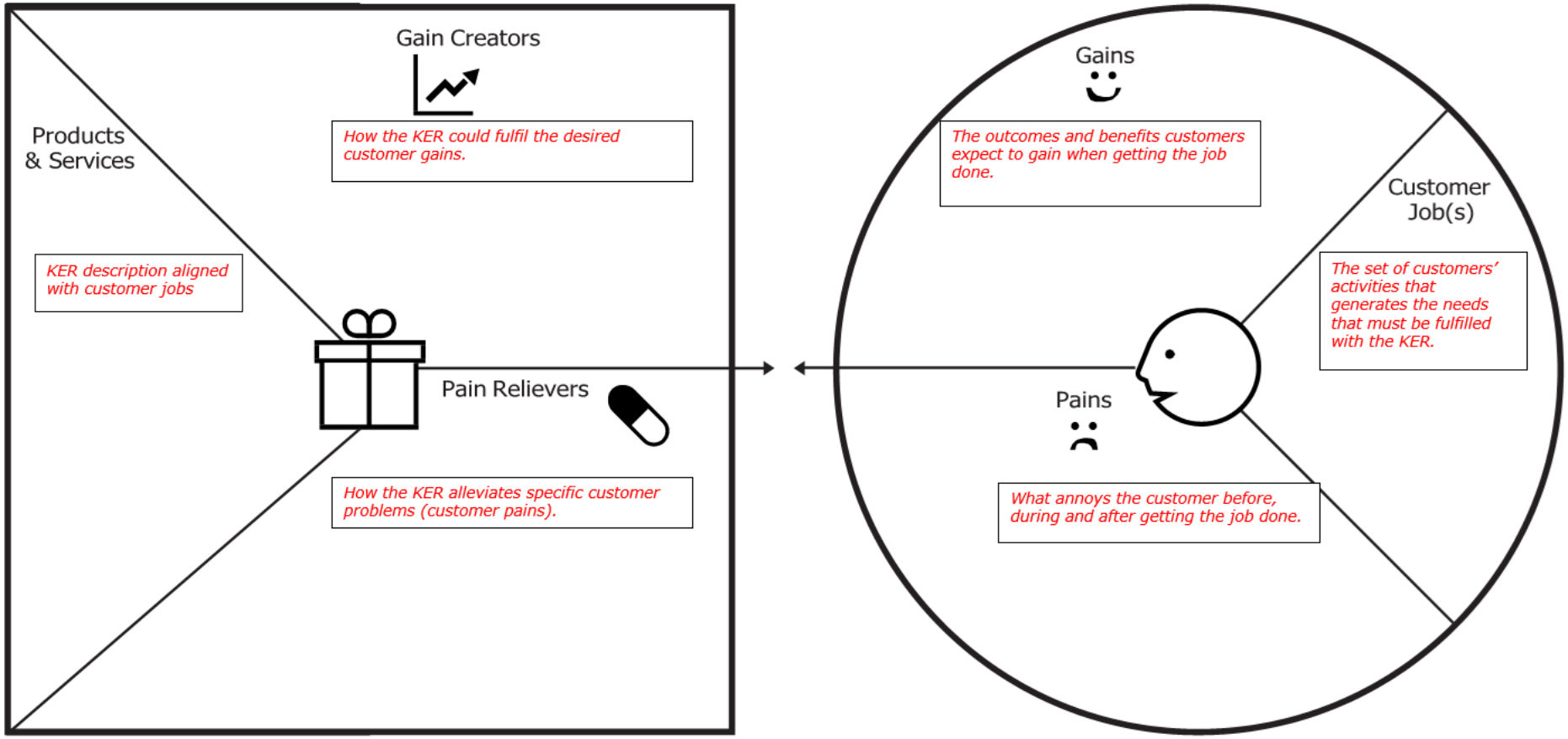


Table 15: The UVP Canvas

MARKET DEFINITION CANVAS

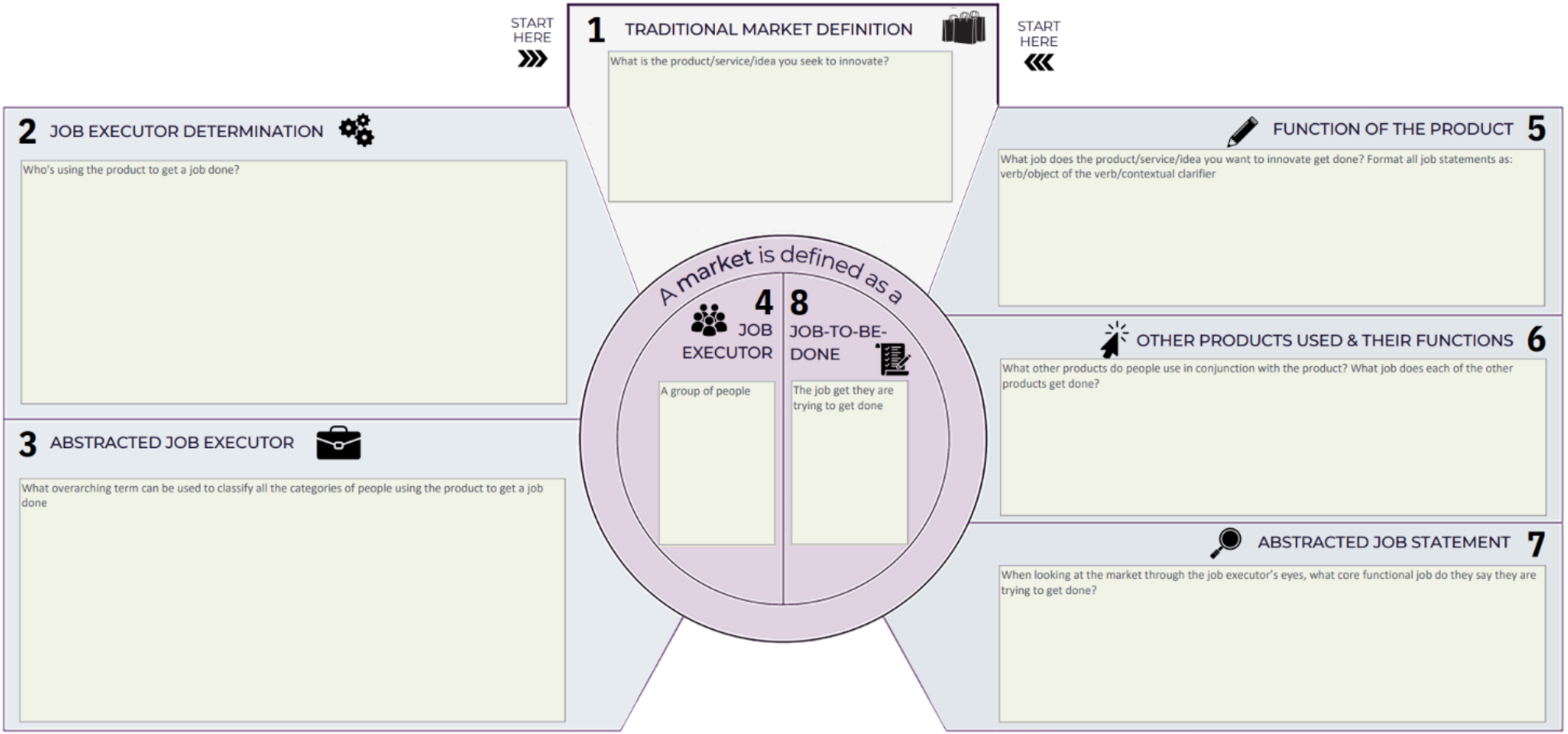


Table 16: The Market Definition Canvas template

6.3.4 Module C: Exploitation strategy

This Module is the third phase of the HRB services and its objective is to develop and/or further improving a high-quality exploitation strategy by revising, complementing, and clarifying existing exploitation plans of the Booster beneficiaries' results and considering the elements linked to the intellectual assets found in the KERs.

This module comprises three templates: The exploitation roadmap (Table 17), the Lean canvas (Table *18*) and the risk assessment map (Table 19).

In brief, the Exploitation Roadmap outlines the concrete steps required to implement the exploitation of each KER after the end of the project. It identifies planned actions, responsible partners, key milestones, estimated costs, expected revenues, and additional funding sources needed to bridge the gap between project completion and market deployment. The Exploitation Roadmap adds value by translating strategic exploitation intentions into a concrete and time-bound implementation plan. It clarifies what actions are required after the project ends, who is responsible for each action, and which resources are needed to move the KER towards market uptake.

Moreover, the Lean Canvas is used to capture the core business logic of each KER in a concise and visual format. It describes the problem addressed, the proposed solution, the unique value proposition, target customer segments, channels, cost structure, and revenue streams. The Lean Canvas provides a structured representation of the business logic behind each KER. It helps validate the market relevance of the result by explicitly linking customer problems to the proposed solution, value proposition, and revenue model.

Finally, the Risk Assessment Map systematically identifies and evaluates risks that may affect the successful exploitation of each KER. It covers technological, market, partnership, legal/IPR, financial, and regulatory risks, assessing their probability, criticality, and potential impact. For each risk, mitigation measures and feasibility of intervention are defined, supporting proactive risk management.

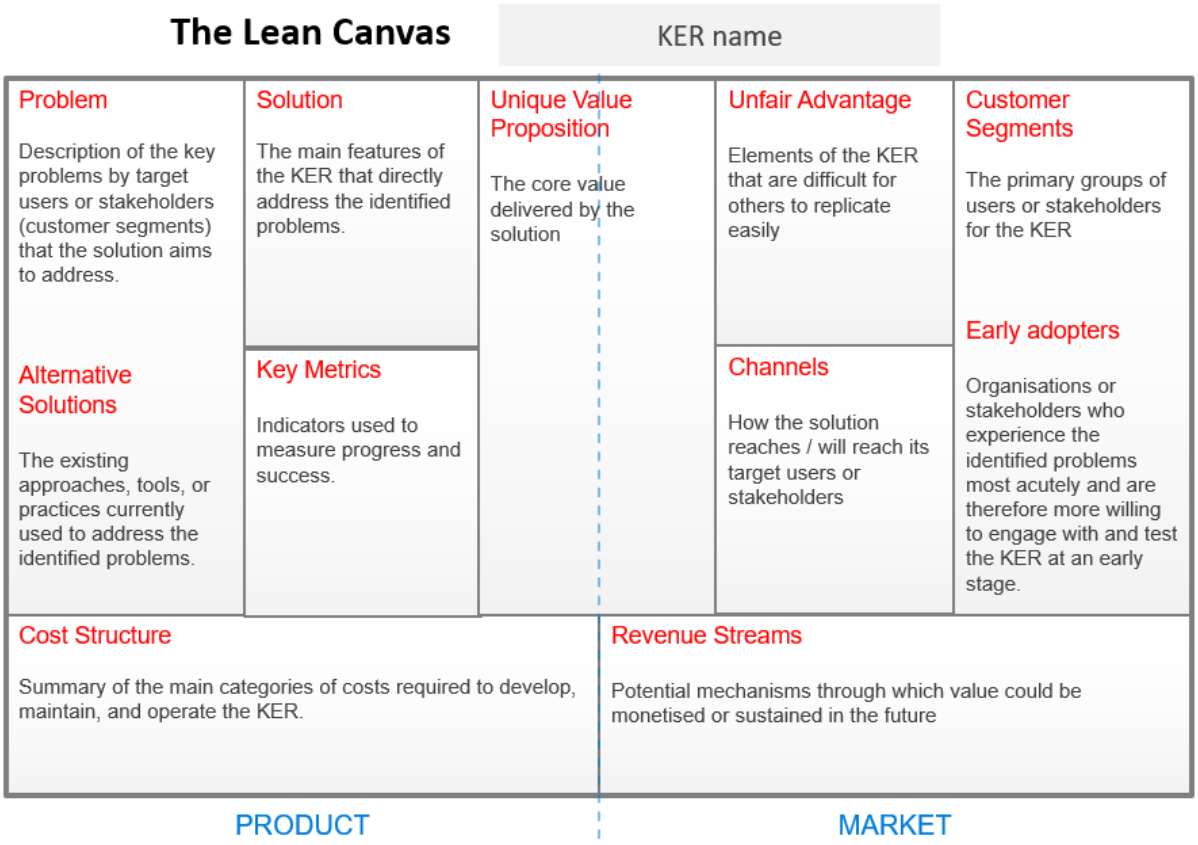
Across the KERs, exploitation strategies converge on a stepwise approach, starting with internal use, further research and dissemination activities, pilot deployments and service-based offerings. In many cases, service-oriented exploitation (e.g. consultancy, integration, validation, customisation) emerged as a more realistic near-term pathway than direct product sales, particularly given the complexity of deployment environments and the need for further research in order to reach higher TRLs. Moreover, another common observation is the continuous ecosystem engagement and collaboration around each KER. For most KERs, effective exploitation is linked to partnerships with network operators, infrastructure providers, vertical industries, research communities and standardisation bodies.

Although no standalone reference model is presented, all templates included in Module C collectively define a reference exploitation model for HORSE, capturing the key actors involved, their interactions and indicative revenue and cost structures across different exploitation pathways. Also, the risk assessment and SWOT analysis (in Module D) reflect some techno-economic considerations, by linking technical maturity, deployment complexity, and integration effort with expected benefits, costs, and exploitation feasibility for different categories of stakeholders.

All templates were completed for each KER, reviewed by either the Booster expert or the project's exploitation manager, and are available at the Appendix D – Module C templates.

Exploitation roadmap	
Actions	Brief description of the actions planned to be executed next year after the end of the project.
Roles	Roles of partners involved in the actions defined above.
Milestones	List of the milestones to be used for monitoring the implementation of the above actions.
Costs	Cost estimation to implement planned activities.
Revenues	Projected revenue streams and eventual profits once the KER will be used. In case the product is under development provide the revenue streams.
Other sources of coverage	Resources needed to bridge the investment needed to increase TRL and ensure the result is used.

Table 17: The exploitation roadmap template



Lean Canvas is adapted from The Business Model Canvas (http://www.businessmodelgeneration.com) and is licensed under the Creative Commons Attribution-Share Alike 3.0 Un-ported License.

Table 18: The Lean Canvas template

Risk Assessment Map

	Description of Risks	Degree of criticality of the risk related to the final achievement of this Key Exploitable Result. Please rate from 1 to 10 (1 low- 10 high)	Probability of risk happening Please rate from 1 to 10 (1 low - 10 high)	Risk Grade	Potential intervention	Estimated Feasibility/Success of Intervention Please rate from 1 to 10 (1 low- 10 high)	Conclusion
	Partnership Risk Factors						
	Technological Risk Factors						
	Market Risk Factors						
	IPR/Legal Risk Factors						
	Financial/Management Risk Factors						

	Environmental/Regulation/Safety risks						

Table 19: The risk assessment map

6.3.5 Module D – The business plan and Module E - Access to other funding & entrepreneurship support

Modules D and E are the final Modules of the HRB service. Briefly, their objectives are:

- To build a business plan that covers essential aspects such as market approach and financial considerations.
- Identification of potential opportunities by other funding programmes and/or additional funding support

The Module D contains one template to be filled, the Business plan (Table 20), while Module E supports Module D (mainly in chapter 9, “The resources”) and does not have its own template to be filled.

The business analysis lies in its focus on the further R&D activities of the HORSE Platform as an integrated and system-level KER, rather than on individual technological components. The platform represents the most significant outcome of the project, as it combines, orchestrates, and operationalises all core technologies developed within HORSE. As such, it constitutes the primary vehicle through which the project’s innovations can achieve tangible technical, operational, and socio-economic impact.

While the business, market, and exploitation analysis has been performed at the platform level, the Business plan does not neglect the individual components of the HORSE architecture. On the contrary, detailed information for all platform main components is included throughout the document, with particular emphasis on future R&D activities and costs.

Overall, the Business plan provides a comprehensive and coherent overview of the HORSE Platform’s exploitation perspective. It includes a consolidated business and market analysis, a SWOT analysis, replicability of the platform, an overview of the business model and go-to-market approach, a structured operative roadmap with joint and individual actions, financial and resource considerations etc.

The template was completed for KER1, reviewed by the Booster expert and is available at the Appendix E – Module D template.

Business plan	
Executive Summary	• This is the introductory section of the Business Plan, as it provides a summary of the future entrepreneurial project. • It clearly, logically, and concisely presents the most relevant information about the company, the goals to be achieved etc.
The organisation	• Provides an in-depth description of the organisation that will lead the exploitation, R&D and other activities of the project, its short- and long-term objectives, strengths and weaknesses and success factors.
The product/service	• This section is dedicated to the description of the HORSE platform, its key components as well as the time to market.

The market	• Describes the target market, its size, stage of development, the barriers to entry, the role that innovation and technological change play in the sector. • A market analysis is included, describing the behaviours and needs of the possible customers and end-users. • The platform's unique value proposition is described and a SWOT analysis is provided.
The business model and marketing strategy	• Describes how the consortium is planning to make money out of the HORSE platform in the future, specifying all different actors involved. • As the aim is to further research and develop the platform as well as to continue the community building around it, this section provides a brief description of the possible use models, channels and pricing strategy that may be applied in the future.
The Team and management structure	• Brief presentation of the key members of the CNIT team that will take care of the R&D, dissemination, fund raising and marketing activities. • Description of the functional responsibilities of the team.
The Operative plan	• A detailed list of activities (either joint or individual) that will start during the next year after the project completion. • Brief description of possible future exploitation paths when the HORSE platform reaches a higher level of maturity.
Financials	• Specification of the financial info for the R&D plan and other activities.
The resources	• This section provides the funding options in order to support the operative plan and cover the costs provided in the financials chapter. • Connection between HORSE and MARE, a follow up HORIZON EUROPE project.

Table 20: The business plan template

6.4 Replicability

Replicability is a key dimension of the impact strategy of the HORSE. In the context of HORSE, replicability refers to the ability to reuse, adapt, and deploy the developed solutions across different operational environments without requiring fundamental redesign or redevelopment. Rather than focusing on a single fixed deployment scenario, HORSE has been designed as a modular, extensible, and platform-based solution, enabling replication beyond the original project use cases.

A central enabler of replicability is the HORSE platform architecture, which integrates multiple interoperable components developed by different partners under a common orchestration and governance framework.

As detailed in Module D of HRB, beyond the core domains of cybersecurity and network security, the replicability of HORSE results extends to a wider range of markets and application domains that share similar requirements in terms of trust, resilience, automation, and orchestration such as healthcare and smart grids. The modular and platform-based design of HORSE can allow easier replication and adaptation to the specific constraints of each market.

From an exploitation and business perspective, Module D highlight that replicability is closely linked to service-oriented and phased exploitation models. Rather than requiring full-scale productisation, HORSE solutions can be replicated through pilot deployments, proof-of-concept installations, and customised integration services targeting specific operators, vertical industries or infrastructure owners.

6.5 Individual exploitation plans

6.5.1 Consorzio Nazionale Interuniversitario per le Telecommunicazioni (CNIT)

Partner Profile

CNIT serves as the coordinator of the HORSE project. As a non-profit consortium unifying 38 Italian public universities, CNIT is positioned as a leading research organization highly active in 5G/6G research and innovation, contributing to the EU's digital transformation goals.

CNIT's competencies lie particularly in network orchestration, virtualization, and DT technology. Within HORSE, CNIT leads the crucial development of the End-to-end Proactive Secure Connectivity Manager (ePEM - KER6), a central component based on the Open-Source MANO orchestrator responsible for securing and coordinating actions over end-to-end services. They are also a co-owner of the overall HORSE Platform (KER1) and jointly own the NDT (KER7) with TID.

CNIT's strategic exploitation focuses predominantly on Research (R) and Internal Use (U), aiming to leverage project outcomes to train young researchers at doctoral and postdoctoral levels and build advanced teaching materials. This institutional commitment enhances their scientific visibility and allows them to influence standardization efforts in groups like ETSI MEC and ENI.

The alignment with HORSE, which promotes a human-centric, sustainable 6G infrastructure, supports CNIT's mission to foster technological excellence necessary for future economic and societal advancements, including those aligned with Industry 5.0 principles.

Exploitation Actions and Expected Return

CNIT's exploitation efforts focus on the knowledge gained and the components where they hold lead or co-lead roles, consistent with their academic mission.

The relevant HORSE results/components include:

- HORSE Platform (KER1/ER6): CNIT is a lead partner for the HORSE platform (KER1), which offers a complete set of features and functionalities towards secure 6G system orchestration. CNIT has an 11% contribution percentage toward KER1.
- End to end Proactive Secure Connectivity Manager (ePEM - KER6/ER11): CNIT is the primary leader for the ePEM (KER6). The ePEM is a central architectural element within the HORSE security infrastructure, responsible for orchestrating actions and providing observability over end-to-end services secured within the perimeter. It is based on the Open-Source MANO orchestrator.
- Network Digital Twin (NDT - KER7/ER12): CNIT is a co-owner, along with TID, of the Network Digital Twin (KER7). The NDT is an environment used for testing "what-if" scenarios and performing predictions on the network state. CNIT has a 50% contribution toward KER7.

As an academic consortium, CNIT's primary target audience is focused on research and education:

- Academic and Research Community: the results will be used to train young researchers at doctoral and postdoctoral levels and educate future research professionals on 6G, and related topics covered by HORSE.
- Students: undergraduate and master's students, extending their courses and introducing new research topics in 6G security and orchestration.
- Standardization Bodies: CNIT intends to disseminate results through presentations in relevant bodies, specifically mentioning ETSI working groups such as MEC, ENI, and IOWN.
- Internal Collaborations: CNIT plans to perform internal dissemination to identify additional synergies within its consortium partners (national universities operating in the telecom area) to foster new ideas and concepts.

CNIT's exploitation scenarios are fundamentally academic, focusing on knowledge transfer and influencing external bodies:

- Education and Training: the core exploitation scenario involves using the project knowledge and results to build teaching material, particularly at the master's and PhD levels.
- Further Research: leveraging the project outcomes and gaining expertise in new research projects and initiatives to further promote research in these areas.
- Technology Transfer (Non-Commercial): presenting and discussing the results achieved in international scientific journals, magazines, and conferences (scientific dissemination).
- Standardization Engagement: dissemination of achieved results through presentations in ETSI working groups (MEC, ENI, IOWN).
- Open Source: CNIT is involved in KERs released under open-source licenses (KER1: Apache 2.0; KER6/ePEM: GPL v3; KER7/NDT: Apache 2.0).

This aligns with CNIT's pathway of being open to handling intellectual property generated during the project according to the rules defined in the Grant Agreement. CNIT typically aims to strengthen its position as a reference partner in the research field. CNIT's declared exploitation type for the HORSE Platform (KER1) is Research (R), and its strategy pathway is Internal Use (U) and Services (S) (e.g., consultancy, training).

The expected returns:

- Economic: CNIT is not primarily focused on direct economic returns, but rather on its core mission.
- Strategic:
  - Strengthening research position: CNIT will strengthen its position as a leading research institution in areas like 6G digital twins and secure proactive orchestration.
  - Increased visibility: increasing the visibility, recognition, and publication record of the University/Consortium.
  - Internal Synergies: fostering the development of new ideas and concepts within the CNIT consortium members to maximize the project's impact.
- Knowledge-based:
  - Expertise acquisition: gaining knowledge and expertise (know-how) from H2020 5G projects, particularly concerning 5G Service Based Architecture and network slicing.
  - Skilled workforce: training future highly skilled professionals (doctoral and postdoctoral researchers) in network management and security for next-generation mobile networks.
  - Improved cybersecurity/edge/cloud integration capabilities: building on CNIT's experience in 5G network orchestration and Digital Twin concepts, leveraging AI to build accurate replicas of physical twins and train AI models.
- Policy / Standardization:
  - Influencing standards: contributing to and influencing the evolution of standards through presentation of results at ETSI working groups (MEC, ENI) and IOWN.

Strategic Future Plans and Commitment

CNIT is the coordinator of the HORSE project. As an academic partner, CNIT's strategic future focus primarily on advancing research capabilities, integrating outcomes into educational programs, and influencing standardization efforts related to 6G security and orchestration.

CNIT's long-term vision centres on leveraging the knowledge and technological assets gained from HORSE to solidify its standing as a leading research institution in next-generation communications and secure, intelligent systems. Also, CNIT is the lead organisation for coordinating further R&D, exploitation and other activities for the KER1 - HORSE platform always in cooperation with the rest consortium partners, co-leader for the previous activities for KER7 – NDT along with TID and leader for KER6 - ePEM.

Concrete exploitation actions:

1. Training and Education Programs (Core Action): the primary goal of CNIT's exploitation plan is to educate future researchers on 6G and related topics covered by HORSE.
   - The knowledge and results obtained will be used to train young researchers at doctoral and postdoctoral level.
   - Specific HORSE topics and results will be used to build teaching material, particularly at the Master and PhD level.
   - The skills inferred from the project will be translated into knowledge to be transmitted within different undergraduate and master's courses and utilized to attract new students to the Computer Architecture PhD program.
2. Further Research and Internal Use: CNIT intends to leverage the outcomes and gained expertise in new research projects and initiatives to further promote research in these areas. CNIT's declared exploitation type for the core HORSE Platform (KER1) is Research (R), with a pathway of Internal Use (U) and Services (S) (like consultancy and training).

3. Standardisation Engagement: CNIT will disseminate achieved results through presentations in different ETSI working groups, specifically mentioning MEC, ENI, as well as IOWN. This effort aims to influence the evolution of standards in areas relevant to HORSE.

As an academic/research consortium, CNIT's "product roadmap" relates to its internal tools, research platforms, and the knowledge foundation provided to external partners.

- Enhancement of Internal Platforms: CNIT will build upon its existing Background IP (BG IP) and Foreground IP (FG IP) components. The prototype developed during the H2020 5G-MATILDA project, which acts as an Operations Support System (OSS) module based on Open-Source MANO (OSM), will be extended, enhanced, and adapted to the HORSE framework. This component is the basis for the End-to-end Proactive Secure Connectivity Manager (ePEM) (KER6).
- Maintenance of Open Source KERs: CNIT is the main partner for the ePEM (KER6), licensed under GPL v3, and a co-owner of the HORSE Platform (KER1) and the Network Digital Twin (NDT) (KER7), licensed under Apache 2.0 and MIT licence respectively. This open-source strategy facilitates long-term maintenance and community involvement, aligning with CNIT's research-focused exploitation pathway ("Further research" is identified as the post-project plan for several CNIT-related BG/FG IPs).

CNIT explicitly engages in joint research and technology ownership with partners, suggesting continuation of these collaborations:

- Joint Ownership: CNIT is a co-owner of the HORSE Platform (KER1), along with UPC, and a co-owner of the NDT (KER7), along with TID. These jointly generated results (which require prior written consent of all co-owners for commercial or developmental activity involving third parties) form the basis for future collaborative exploitation.
- Internal Synergies: CNIT plans to perform internal dissemination to identify additional synergies within its consortium partners (national universities operating in the telecom area).
- Open Collaboration: CNIT contributes to fostering an open, standardized solution ecosystem.
- Joint actions with third parties: CNIT is always open for new collaborations and joint activities with third parties regarding the components developed within HORSE. For KER7, Trentino Digitale S.p.A. has already expressed their interest for further actions (see Appendix F – Letter of support).

CNIT’s commitment is institutional, manifesting primarily through human resource allocation to training and research:

- Human Capital: CNIT will dedicate resources toward training future highly skilled professionals (doctoral and postdoctoral researchers) in 6G security and orchestration.
- Infrastructure/Platforms: Continued use and enhancement of its internal testbeds and software tools, such as the NFVCL and MetalCL, which were utilized for the HORSE components and are intended for further research.
- Project Management: CNIT serves as the Project Coordinator (WP1 lead), demonstrating a strong central commitment to the project's overall successful execution and legacy.

HORSE directly aligns with CNIT’s mission as a leading research consortium in ICT and telecommunications:

- 6G and Digital Transformation: CNIT is active in 5G/6G research and brings expertise in Digital Twin concepts and network orchestration. HORSE's overarching goal is to address the complexities of 6G, including secure service provisioning and trust, which are central to the concept of digital transformation.
- Industry 5.0/Sustainable Economy: HORSE promotes a human-centric, open-source, green, sustainable coordinated provisioning and protection platform. This focus on sustainability, resilience, and human-centric design aligns with the principles of Industry 5.0 and the broader European Green Deal, as HORSE aims to enable secure services while jointly optimizing the carbon footprint and resource utilization.
- Expertise Development: the project's outcomes strengthen CNIT's capabilities in key areas like 5G Service Based Architecture, network slicing, and Digital Twin concepts, leveraging AI to create accurate replicas of physical systems.

6.5.2 Telefónica Innovación Digital (TID)

Partner Profile

Telefónica Innovación Digital (TID) is a wholly-owned subsidiary company of Telefonica, S.A. (parent company of the Telefonica Group) committed to carrying out the Research, Development, and Innovation (R&D+I) activities in the field of telecommunications, telematics and information systems, as well as to nurturing the Telefonica Group with the necessary support elements for its development. These activities are primarily directed, though not exclusively, towards the study and preparation of documentation for Product Development, Exploratory Development, Applied Research, Technological Reports, Situational Studies on techniques and technologies, Testing Services, Quality Control, and Audits.

Among the most relevant activities of the company are the following:

- The specialization, or cooperation, and the exchange of scientific and technological information and knowledge either through the creation of joint ventures or participation in consortia with third-party companies
- Provision of technical assistance services, professional training, as well as the exchange of scientists, engineers, and other specialists.
- Maintenance of technological and commercial knowledge under any form of legal protection, including industrial or intellectual property.
- Organization of seminars and other events on specific topics related to the communications sector and information digital technologies.
- The undertaking of joint research projects with cost sharing and work distribution under specific agreements.
- Participation in sponsoring activities jointly with universities and other public institutions, both national and international.
- Engagement in activities and providing services in the areas of telecommunications, information society and communication services
- Investment activities in the communications and information technology sector in the broadest sense, at the national and international levels, through the acquisition or participation in the capital of national or foreign companies established or to be established in this sector.

Exploitation Actions and Expected Return

TID's exploitation strategy has focused on the role of the company within the Telefonica Group, focusing on building awareness of the project results to become integrated within the strategic roadmap of the relevant Telefonica business units in Europe and the world, focused on the enhancement of infrastructure security and the support for enhanced services to customers.

In particular, the application of AI and NDT technologies for cybersecurity assessment and remediation strategy evaluation has constituted the core of TID's exploitation actions. These results have also been introduced the entrepreneurship initiatives of Telefonica (Wayra and Telefonica Open Future) with the goal of facilitating their application by the start-ups nurtured by these initiatives.

With this main technology targets in mind, TID has communicated, promoted and demonstrated the within the Telefonica Group units working in network architecture evolution, management automation and Cybersecurity services, and especially with our division for added-value network services, Telefonica Tech. TID has shared project outcomes, especially open-source results and demonstrators, with relevant Telefonica research and industrial partners in the security community, cooperating with them to transfer process to the Telefonica innovation and industry ecosystem at large.

Taking advantage of project demonstrators, and especially of the work related to the ETSI ZSM PoC, Telefonica's business units are evaluating how to incorporate the project results to their commercial services, mainly by improving their cybersecurity planning and assessment procedures applying HORSE design patterns and tooling concepts, and the standards that have evolved by means of project contributions to relevant SDOs.

Standardization activities have been TID's key target for addressing exploitation, as they are a key element for telco activity, whether in terms of service design, purchase decisions and regulatory compliance. TID has acted as the main standardization agent for HORSE results, leveraging project outcomes to lead and contribute to different activities in relevant SDOs such as ETSI, IETF and 3GPP, as already reported in previous deliverables and in the corresponding section of this one.

Strategic Future Plans and Commitment

TID intends to continue the exploitation activities along the lines described in the above section, in particular continuing the consolidation of HORSE outcomes in the Telefonica business units, progressing with the standardization lines that the project has supported, and using HORSE results as the foundation for further research and innovation work, especially focused on 6G technologies. More specifically, TID is co-leader in KER7 – NDT and will be responsible for leading the future R&D, exploitation and other activities in cooperation CNIT.

TID will seek the consolidation of the procedures, design patterns and tools developed in HORSE within the Telefonica business units, leveraging these results via the interactions with the technical teams of these business units and, most importantly, in the collaboration with other actors on the Telefonica technology ecosystem: researchers, vendors, integrators and start-ups.

Standardization timeframes do not match with project lifetimes, and are usually longer than them. TID has a strong commitment to continue the standardization paths that have been started and/or supported by HORSE. This obviously includes leveraging the leadership positions that have been achieved. Work on NDT, telemetry data, security management, data infrastructures and other aspects will continue as a natural extension of HORSE exploitation goals.

Finally, HORSE has provided TID an excellent background to continue working on research related to AI-enabled, evidence-supported security management, with a specific focus on the development and deployment of 6G. An immediate result is the successful start of project MARE, where several of the principles developed in HORSE will be extended. Furthermore, several proposals related to the applicability of NDTs an evidence-supported security management have been submitted by the time of writing this document.

6.5.3 Ericsson Telecomunicazioni Spa (ETI)

Partner Profile

Ericsson is a global leader in the telecommunications sector, operating in over 180 countries with a workforce of approximately 101,000 employees. The company has a long-standing commitment to research and development, with around 30% of its personnel engaged in R&D activities. In recent years, Ericsson has significantly increased its investment and human resources dedicated to the research, definition, and development of new products, with a total global expenditure of approximately 42 billion SEK (over 18% of its revenue, involving about 27,700 employees). This commitment has yielded world-class results, establishing Ericsson as a recognized technological leader across the telecommunications industry.

The company holds one of the most comprehensive and extensive patent portfolios in the sector, with over 60,000 patents, around 400 of which have been developed by researchers in Italy over the past eight years. Many of these patents are licensed through non-discriminatory agreements based on fairness and reasonableness, promoting sector-wide technological development, enabling new market entrants, and preserving Ericsson's own capacity for continued innovation, including through open standards. This approach demonstrates Ericsson's leadership not only in innovation but also in fostering collaborative progress within the telecommunications industry.

Ericsson's research and innovation have enabled mobile broadband communications, which today underpin advanced technologies such as cloud computing, smart grids, machine-to-machine communications, Internet of Things (IoT), and mobile commerce. In Italy, Ericsson Telecomunicazioni S.p.A. focuses on high-value R&D areas with multi-technology competencies and global product responsibilities. The company's Italian R&D division, comprising over 600 employees, is organized into operational units located in Genoa, Pagani, and Pisa. These units possess the expertise, human resources, and testing methodologies necessary to carry out all types of R&D activities related to the company's products and technologies.

The Genoa R&D center, with more than 340 staff, is distinguished by its responsibility in several critical areas: security within the Ericsson Network Manager (ENM), Software Defined Network solutions and zero-touch operations for Operational Support Systems (OSS), FrontHaul solutions, and the application of software technologies to telecommunication systems design. Technologies employed include Java, C++, Scala, GO, Python, Plex, Docker, Linux, Windows, Solaris, Oracle, and Sybase, alongside third-party tool integrations. The center is a pioneer in adopting Component-Based Architecture (CBA), implementing microservices architectures that are highly scalable and cloud-native, providing modular, flexible, and dynamic solutions capable of supporting diverse applications beyond telecommunications. Furthermore, Ericsson applies Agile methods, Lean management principles, and DevOps product lifecycle management to ensure continuous and close collaboration between development and IT operations.

Ericsson's strategic focus is on technological leadership, positioning the company at the forefront of communication systems development across all sectors—from traditional fixed telephony networks to next-generation IP, broadband, GSM, GPRS, UMTS, LTE, and 5G networks. The company operates through four segments: Networks, Digital Services, Managed Services, and Emerging Business and Other. This organizational structure allows Ericsson to design, implement, and manage advanced network solutions, cloud-native software, AI-driven operational services, and innovative enterprise technologies. Unlike other European manufacturers tied to their domestic markets, Ericsson has maintained an international vision since its founding in 1876, today operating in more than 1,000 networks across 180 countries, generating approximately 96% of its revenue outside Sweden. Ericsson's Italian presence, dating back to 1918, includes strategic partnerships with major

operators such as TIM, Wind-Tre, Fastweb, Vodafone, and Tiscali, as well as a wide network of qualified partners nationwide.

Within the HORSE project, Ericsson has played a pivotal role across all activities, from initial state-of-the-art studies and benchmarking to requirements definition, architectural design, demonstrator development, and impact creation, communication, and dissemination. Notably, Ericsson led a critical Work Package, the HORSE Intelligence, coordinating five essential tasks that form the “brain” of the project framework. Among these, Task 5 focused on developing a machine learning-based threat detector, a truly innovative solution entirely designed, implemented, and integrated by Ericsson. This involvement leverages Ericsson’s core competencies in AI model development, cloud and edge computing infrastructure, system integration, and software design, demonstrating the company’s ability to contribute technological expertise to complex, cutting-edge research initiatives.

Ericsson’s engagement in the HORSE project exemplifies its ability to combine innovation, digital transformation, and technological leadership to deliver tangible outcomes. By applying its deep expertise in AI, microservices architecture, cloud-native systems, and advanced R&D processes, Ericsson has not only strengthened the project’s technical capabilities but also ensured that its outputs are scalable, secure, and adaptable to evolving telecommunications and industrial requirements. Through its contributions, Ericsson is helping to shape a future in which intelligent, automated, and highly secure systems can respond to increasingly complex operational and security challenges, aligning perfectly with the objectives of HORSE.

Exploitation Actions and Expected Return

The core Key Exploitable Result (KER) for Ericsson within the HORSE project is the DEME (Detection Engine and Mitigation Engine), an innovative machine learning-based threat detector. Unlike traditional solutions, which operate within isolated silos and thus have limited visibility, DEME employs a hierarchical tree structure that aggregates the outputs of successive processing steps. This design overcomes the “siloization” problem typical of conventional threat detectors, enabling the identification of anomalous or previously unknown (0-day) attacks across multiple domains. The unique architecture of DEME allows it to consolidate and analyze information from multiple parallel detectors, providing a comprehensive situational awareness that enhances detection accuracy and resilience.

From a market perspective, the DEME sub-system is highly relevant to Ericsson’s product portfolio, particularly within the domain of next-generation Operational Support Systems (OSS). By integrating this advanced detection and mitigation engine as a core feature in Ericsson’s OSS solutions, the company can significantly enhance the attractiveness, competitiveness, and technological differentiation of its offerings. Target markets extend beyond the conventional SIEM and network management devices to include broader network solutions where security and anomaly detection are critical. These solutions are aimed at telecommunications operators, enterprises managing complex network infrastructures, and critical service providers that require advanced, AI-driven cybersecurity capabilities.

The exploitation scenario for the DEME sub-system involves direct integration into Ericsson’s OSS portfolio as an advanced, value-added feature. The deployment strategy will possibly leverage Ericsson’s existing customer base, ensuring rapid adoption within operational networks and providing a clear pathway to market.

Expected returns from this exploitation are multi-dimensional. Economically, new OSS generations with new evolved features like DEME are expected to generate new revenue streams and improve the competitiveness of Ericsson’s OSS products, contributing to the broader network solutions market. Strategically, these new solutions will confirm the Ericsson position as a leader in 6G-era network security, expanding the company’s service portfolio and reinforcing its technological leadership. Knowledge-based returns include enhanced capabilities in cybersecurity, AI-driven detection, and edge/cloud integration, strengthening

Ericsson's internal expertise and innovation potential. From a policy and standardization perspective, the adoption of the DEME innovative ML architecture in Ericsson's commercial solutions may enable the company to influence European cybersecurity regulation, contributing to the definition of industry standards for AI-enabled threat detection and network security.

Overall, the exploitation of evolved Machine Learning features like DEME represents a strategic convergence of technological innovation, market relevance, and long-term positioning, aligning Ericsson's core competencies with emerging cybersecurity needs and supporting the company's ambition to deliver next-generation, intelligent, and highly resilient network solutions.

Strategic Future Plans and Commitment

Ericsson's medium- to long-term vision for sustaining and building upon the HORSE outcomes is centered on the strategic integration of the DEME (Detection Engine and Mitigation Engine) feature into its future OSS (Operational Support Systems) product roadmap. The DEME engine represents a highly innovative and high-performing component that has the potential to significantly enhance the competitiveness of Ericsson's OSS portfolio, thereby strengthening the overall attractiveness of the company's end-to-end network offering—from the radio access segment through to the core. This aligns with Ericsson's broader strategic objective of delivering secure, intelligent, and high-value solutions across its entire network ecosystem.

However, Ericsson's innovation landscape is extremely rich, with substantial investments in R&D, thousands of active research projects, and a continuous flow of new patents each year. As a result, the integration of novel features such as DEME must be carefully assessed and prioritized within the company's extensive innovation pipeline. Product features are typically selected based on their technological maturity, market demand, and strategic fit, as well as on direct input from key customers and Business Areas (BAs). Therefore, while DEME is already recognized for its innovative potential, its inclusion in upcoming OSS releases will depend on a structured internal evaluation and prioritization process.

The Ericsson R&D department that contributed to the development of DEME plays a consultative and facilitative role in this process. Now that the solution is fully functional, integrated, and supported by demonstrable Proofs of Concept (PoCs), the department is responsible for promoting the feature internally to relevant BAs and Customer Units (CUs). This involves organizing systematic innovation events that bring together representatives from R&D, BAs, CUs, and major clients to collect feedback, assess interest, and support decision-making regarding the inclusion of the feature in future product lines.

Concrete post-project exploitation actions include continuous internal demonstrations, integration testing within Ericsson's development environments, and participation in innovation and co-creation initiatives. DEME was already presented at Ericsson's Innovation Day in autumn 2025 and is scheduled for a live demonstration during the next event in June 2026, where practical showcases will be used to validate interest and potential market adoption. These actions are part of a broader institutional commitment to ensuring that promising HORSE outcomes are effectively transitioned from research prototypes to commercial-grade solutions.

In the long term, the exploitation and evolution of DEME directly support Ericsson's strategic priorities and corporate mission, which focus on digital transformation, intelligent automation, and the advancement toward Industry 5.0. By maintaining and scaling the HORSE outcomes, Ericsson reinforces its position as a global technology leader, committed to delivering secure, adaptive, and intelligent network solutions that anticipate the needs of future communication ecosystems.

6.5.4 Technische Universitaet Braunschweig (TUBS)

Partner Profile

Technische Universität Braunschweig (TUBS) is a renowned technical university founded in 1745 and a member of the TU9, a group of Germany's leading technical universities. As a technical university, TU Braunschweig focuses on a wide range of engineering fields, including architecture, electrical, mechanical, civil, and environmental engineering, as well as computer science. Scientists at TU Braunschweig address future-oriented key scientific and societal issues through interdisciplinary research centers that work across faculties and with non-university institutions and industry. The research team in HORSE Project belongs to the Institute of Computer and Network Engineering (IDK). In the project context, TU Braunschweig is responsible for the research and implementation of network tools focusing on automation and intent-based management, such as the HORSE Intent-based Interface (IBI). TU Braunschweig members participating in the HORSE project have a strong background in computer networks, network management, and security, both in research areas and real network deployments.

Exploitation Actions and Expected Return

As an academic partner, TU Braunschweig's primary focus is on training students, mainly doctoral and postdoctoral researchers, in technologies relevant to advanced 5G and 6G network management. Therefore, the technologies researched and applied in HORSE could be used to extend bachelor's and master's courses by introducing topics relevant to the management and security of next-generation mobile networks, as well as inspire the writing of PhD dissertations and prepare new professionals to work on those topics.

From a research perspective, participation in HORSE enhances TU Braunschweig's research profile by encouraging students and researchers to collaborate with academic and industrial partners. The collaborative work allows them to incorporate new technologies and scientific advancements from HORSE into their publications, thereby enhancing the scientific standing of the personnel involved. The development of the IBI module within the HORSE framework has already spurred research on combining intent-based networking and digital twins to assess and improve autonomous solutions for the management of communication networks.

Strategic Future Plans and Commitment

TU Braunschweig (TUBS) views its participation in the HORSE project as a core component of its long-term strategy to establish itself as a leading research institution in next-generation communications and secure, intelligent systems. In this context, TUBS will further explore the knowledge and experience gained during the HORSE project in other research projects focusing on network security and autonomous networks. Key personnel involved in the HORSE Project will be retained or redirected to follow-up research initiatives. This includes continued effort by the involved institute to integrate the theoretical and practical results (e.g., advanced orchestration algorithms for autonomous networks and 6G security mechanisms) into future research proposals.

The IBI module developed within the HORSE project framework will serve as background knowledge for other research initiatives, providing a starting point for more complex solutions. The expertise gained in HORSE will be applied to tools for autonomous network management and security orchestration. TUBS also plans to apply the knowledge gained from HORSE to standardization activities and to collaborate with technology recommendation bodies.

6.5.5 Ethniko Kai Kapodistriako Panepistimio Athinon (NKUA)

Partner Profile

The National and Kapodistrian University of Athens (NKUA), officially founded on April 14th, 1837, is the largest University not only of Greece but both of the Balkan peninsula and of the Eastern Mediterranean region. It has 2.100 permanent faculty members and 40.000 undergraduate students. NKUA is ranked 58th among all European Union Universities and 257th in world ranking. Within the HORSE framework, NKUA is responsible for the development of AI/ML approaches for security protection within the HORSE platform, as well as for the development of the distributed AI trustable engine (DTE). All members of NKUA participating in the HORSE project have a strong background on the development of ML approaches for various tasks (i.e., threat mitigation, service improvement, etc) related to 5G/6G networks.

Exploitation Actions and Expected Return

NKUA foresees three important routes towards exploitation of the results. The first focuses on exploiting HORSE results in education; the second focuses on enriching the scientific status of the involved personnel; and the third one is aimed at exploiting the project outcomes in future research projects and in general other markets. On the first exploitation strand, HORSE will help extend the undergraduate and MSc courses, while introducing new research topics on the field of 6G security and secure orchestration of highly demanding applications with AI/ML approaches, for the creation of modern and innovative PhD Dissertations.

With respect to the second exploitation strand, NKUA sees the participation in HORSE as a clear step towards the exploitation of the technical and scientific advancements, which will be developed in close collaboration with the rest of the project partners. The interest is mainly focused in the areas of physical layer security and AI where the involved personnel have a remarkable research record and relevant publications. To this end, NKUA has already accomplished the task of implementing DTE within the framework of HORSE. As a next step, NKUA foreses to leverage the mechanism of distributed AI via the introduction of the KER Distributed AI for Services Preassessment. This KER aims to effectively engage the minimum number of available resources in a 6G network for proper service execution. It relies on proper model training in a federated fashion way by taking into consideration various performance metrics, such as service complexity, hardware resources, security policies, etc.

Strategic Future Plans and Commitment

With respect to the third exploitation field, NKUA will leverage the outcomes of this project and build upon the gained expertise to be exploited in new research projects that would give the opportunity to further promote research in these areas. The NKUA involvement in a highly innovative project with industrial partnerships will allow its establishment as a significant European research and development organisation and it will increase the visibility, recognition, and publication record of the University. Therefore, NKUA will stay competitive for future research projects and initiatives and strengthen its position as a university (knowledge, scientific quality, facilities). This is the core of individual exploitation plan.

In particular, and with respect both to the DTE as well as the Distributed AI for Services Preassessment, the target market mainly refers to 6G network providers or other beneficiaries who make use of 6G resources, e.g. smart grid market users. To this end, both DTE as well as the related KER can offer competitive advantages, such as optimum resource allocation in complex environments, such as the 6G framework, which are based on the integration of various heterogeneous resources. NKUA plans to organize webinars and dedicated sessions to industrial partners to further promote the aforementioned outcomes and identify potential additional stakeholders.

6.5.6 Suite5 Data Intelligence Solutions Limited (S5)

Partner Profile

Suite5 (S5) is an Information Technology Solutions and Services SME whose mission is to deliver innovative data-driven intelligence solutions through state-of-the art technologies, required for any organization to be placed at the forefront of competition through greater efficiency. By combining strong technology know-how and hands-on approach in managing and implementing projects commissioned by the public and the private sector, S5 provides research-inspired solutions and practical support for its clients in order to leverage business and crowd intelligence into their everyday operations.

Exploitation Actions and Expected Return

S5, through the development, deployment and validation of the PAG component, acquired further technological and innovation know-how related to 5G/6G applications, which shall further complement its existing tools and services portfolio of data-driven intelligence. The integration of the PAG component with other HORSE components (such as the Smart Monitoring) allowed S5 to experiment on and implement new encryption, anonymization and data observability techniques, which in turn shall further expand the capabilities of the S5 Enterprise Analytics software.

Strategic Future Plans and Commitment

The results of S5 work in the HORSE project shall upgrade its services portfolio of data-driven intelligence with 5G/6G specific technological and innovation know-how, and could extend in further research in the future. S5, as a full member of 6G-IA, also targets to focus on the provision of AI-based services to mobile network providers in the future. The exploitation of the results and of the work performed inside the HORSE project shall help gain insights into emerging innovation areas and business models applied on 5G/6G networks (primarily related to AI technologies) and upgrade S5 services portfolio with 5G/6G specific technological and innovation know-how.

6.5.7 Universitat Politecnica de Catalunya (UPC)

Partner Profile

UPC (Universitat Politècnica de Catalunya) is a public institution of research and higher education in the fields of engineering, architecture, sciences and technology, and one of the leading technical universities in Europe. Every year, more than 6,000 bachelor's and master's students, more than 500 doctoral students graduate and 3,067 graduates in lifelong learning. The UPC has a high graduate employment rate: 93% of its graduates are in work and 76% find a job in under three months. Nowadays, UPC offer includes 67 bachelor's degree, 101 master's degree, 46 doctoral porgrammes, supported by 3.703 teaching and research staff filing 23 patents the last year.

Exploitation Actions and Expected Return

UPC, as an academic institution centers its gravity focus on activities related to competences, and knowledge raising, supported by training tasks offered to the distinct level of students along the different academic levels the UPC team involved in the HORSE project show teaching duties. These activities are focused on the different components UPC has played a significant role within the design and development activities, such as the Early Modeling and the Distributed AI Engine, particularly analysing how the different attacks may be modeled to facilitate the preliminary pre-assessmet in emulated contexts (i.e., Sandbox), as well as

identifying specific AI-assisted strategies to support predictive approaches, respectively. Moreover, UPC is co-lead partner for the HORSE platform (KER1), which offers a complete set of features and functionalities towards secure 6G system orchestration. UPChas an 11% contribution percentage toward KER1.

In addition, one of the key contributions of UPC in HORSE is the B5G testbed used for validation purposes. The potential the testbed may have is considered extremely high, when analysing that any new solution in the 6G field should be properly analyzed and validated before being deployed.

Consequently, the exploitation strategy is primarily focused on both the so-called academic exploitation aimed at inferring new knowledge to be shifted into the different subjects the UPC team teaches at, as well as to the strategy to exploit KER1. However, as a key contributor in the project, UPC would join any potential commercial-based strategy set within the consortium where UPC's contribution is relevant.

Strategic Future Plans and Commitment

UPC's main vision when dealing with exploitation resides on academic purposes with a clear target identified on the different student levels. However, as also said above UPC is also open to accommodate any joint activity that may come out from HORSE activities.

6.5.8 EFACEC Engenharia e Sistemas SA (EFACEC)

Partner Profile

EFACEC Group has several Business Units under engineering activities, and EFACEC Transports is one of them.

EFACEC Transports has developed activities in the public transportation market with an important task under ID innovation and development for several projects around the world in implementation of control rooms for TRAMWAYS, Railways and TRAMBUS networks. EFACEC Transports is a technological leadership in all projects involving highly integration with digital solutions and replacing legacy analogue solutions like signaling into a secure digital transformation.

EFACEC Transports' initial aim was to supply to HORSE project an environment to test and validate solutions to detect and control networks that are under attack. Due to some operational challenges (normal when dealing with critical infrastructures), the environment used in the validation process was emulated into B5G testbeds deployed in two academic partners in the consortium. In this context EFACEC Transports' contribution was fundamental to ensure the emulated environment accurately mirrors the real operational infrastructure in EFACEC.

The scenario to be emulated should represent the real context envisioned as the following. EFACEC Transports supplies client software modules that are integrated under 5G/6G network, protected by the HORSE Solution. Through a VPN connection, these client software modules communicate with EFACEC servers and databases, to show information into a Control Room to manage the TRAMWAY network. Typically, all solutions provided by EFACEC are using fiber optics networks to access remote stations and signaling systems across the TRAMWAY network. With 5G/6G HORSE project solution, EFACEC projects could be deployed with a new technological solution that would provide access to remote locations with wireless communications with security tools in the communication channels of the system. The key functionalities of this scenario are emulated into the two testbeds (UMU and UPC) along with the attacks to be used for HORSE validation purposes.

Exploitation Actions and Expected Return

The exploitation plan is the following:

- The HORSE components Threat Detection and Mitigation Engine would allow TRAMWAY Client - Server System to work with security over 5G/6G public networks.
- EFACEC would target the following markets: Public Transportation Projects like TRAMWAYS, Railway and TRAMBUS.
- EFACEC exploitation scenarios would be a go-to-market strategy or in partnership with public client projects for transportation.

The expected returns will be:

- Economic - projects would have lower costs than using fiber optics installation.
- Strategic - projects 5G/6G technologies with IA based Cyber Security would be considered an advanced technology leadership for client projects.
- Knowledge-based - using an integrated system that joins wireless high-speed networks and cyber security tools in one solution opens the product line available for client projects and the implementation knowledge of this system when compared with legacy fiber optics networks.

Strategic Future Plans and Commitment

EFACEC Transportation organisation in a medium to long term vision expects to consider that the HORSE outcomes to be deploy/integrate in new final client projects for Public Transportation and to refurbished older projects that need to be updated in terms of technology.

EFACEC Transportation organization will evaluate a possible Business Case for the HORSE solution integration to apply in TRAMWAY projects. This requires Financial and market analysis to be done after the R&D project completion.

The knowledge and evidence that the HORSE solution works and has positive feedback from deployment in HORSE Use Cases is to be consider in proposals for new client projects and updates for older projects has a solution to be presented by EFACEC commercial teams

6.5.9 HOLO-Industrie 4.0 Software Gmbh (HOLO)

Partner Profile

Founded in 2015, Hololight has emerged as a global leader in augmented and virtual reality softwares for the enterprise market. By collaborating closely with technology, networking, cloud, software, and hardware partners, as well as industry organizations, Hololight has built a robust ecosystem. The company provides XR software, infrastructure, and streaming technology to visualize and manage industrial 3D data at scale, revolutionizing how companies engage with 3D content and scaling XR use.

Hololight is a use case leader in HORSE, a project showcasing how emerging 6G technologies can enable smart, secure, and adaptive network services across interconnected systems. HORSE focuses on advancing 6G infrastructure for intelligent connectivity, computing, and security management. Within this framework, Hololight exploits the HORSE platform-next-generation 6G network capabilities-to deliver robust, low-latency, and secure XR experiences. This includes the visualization and manipulation of complex 3D CAD files remotely through Hololight Space, empowering engineers and designers to collaboratively review digital twins, optimize factory layouts, and perform virtual prototyping in real time. By integrating Hololight Stream, an advanced XR streaming SDK, Hololight overcomes the limitations of conventional

standalone XR devices—such as limited processing power and display resolution—by offloading rendering to high-performance servers or cloud environments. Leveraging the HORSE platform's strengths in edge computing, programmable networking, and AI-based security, Hololight ensures seamless, high-fidelity visualization and data protection across devices. Through this collaboration, Hololight demonstrates how 6G-enabled infrastructures can unlock the full potential of immersive, industrial XR applications.

Exploitation Actions and Expected Return

HOLO is utilizing the following HORSE components for the use case- "secure remote rendering for XR collaboration".

1. **Infra** – the testbed to deploy 5G core and HORSE components
2. **Smart monitoring tool** for collecting the traffic data from the infra for the prediction/detection/mitigation.
3. **Preprocessing tool** for normalizing the data collected by the Smart Monitoring tool.
4. **DEME** for detecting cyber-attacks.
5. **DTE** for employing AI/ML modules to define the optimum set of policies that leverage security against all potential attacks.
6. **IBI** for enhancing user engagement and facilitating the automation of decision-making within the network management system.
7. **cKB** is a repository and dynamic resolver for information related to threats, mitigation strategies, and security intelligence.
8. **CAS** for ensuring that all security solutions and policies implemented by the HORSE platform adhere to the necessary regulatory and ethical standards.
9. **RTR** for threat mitigation.
10. **ePEM** for enabling a secure and resilient 6G wireless and computing ecosystem through service orchestration.
11. **DOC** as the crucial SouthBound Interface for the ePEM, integrating the physical and virtual infrastructure elements into a unified resource stratum.

The threat detection and mitigation tools are relevant for HOLO for research and innovation purposes. HOLO has end users across manufacturing, construction and defence industries where remote collaboration on designing, prototyping and reviewing is crucial. Making this use case cyber secure enhances the utility and the market value of the technology. The mature product will be licensed to the end-user industries.

Incorporating the research outcomes of HORSE into HOLO's XR technology has many benefits. From an economic perspective, the integration is expected to generate new revenue streams through secure XR services and licensing opportunities, while improving product competitiveness in high-value industrial markets. Strategically, this collaboration will strengthen HOLO's positioning within the emerging 6G security ecosystem, enabling advanced cybersecurity in immersive technologies. On a knowledge level, it will enhance HOLO's awareness in cybersecurity for XR (which otherwise is not easily accessible), as well as in edge and cloud integration for secure, low-latency applications. Finally, from a policy and standardization standpoint, participation in HORSE-related research will allow HOLO to contribute to and influence ensuring that XR security requirements are represented in future regulatory developments.

Strategic Future Plans and Commitment

HOLO has greatly benefited from HORSE by gaining valuable knowledge and awareness of cybersecurity requirements and their benefits, which has strengthened its capability to design secure and resilient XR solutions. The research has also made HOLO future-ready for 6G technologies and their integration into industrial XR, keeping the company at the forefront of

innovation and market competitiveness. Building on these outcomes, HOLO will integrate HORSE's threat detection and mitigation tools into its XR collaboration platform, develop new secure XR services, and initiate targeted cybersecurity training programs. HOLO is open to joint initiatives with HORSE consortium partners for future research to advance products to the next generation of technologies.

6.5.10 ZORTENET Idiotiki Kefalaiouxiki Etaireia (ZORTE)

Partner Profile

ZORTENET is a research-driven Greek SME based in Athens, specialising in advanced ICT solutions for 5G and emerging 6G networks, Network Function Virtualisation (NFV), Software Defined Networking (SDN), trust technologies, blockchain and cybersecurity. The company combines strong R&D capacity with practical experience in systems integration and software development, actively participating in European collaborative projects under Horizon Europe and related programmes, including HORSE, SEPTON, TRUSTEE and EVOLVED-5G.

Within this ecosystem, ZORTENET focuses on secure, programmable and data-driven network solutions that bridge state-of-the-art academic research with industrial-grade platforms, contributing expertise in network monitoring, anomaly detection, trust management and distributed ledger-based mechanisms. Its role in HORSE builds directly on this profile, positioning ZORTENET as a key contributor to the development and validation of a 6G-ready, security-aware infrastructure where connectivity, computing and security are treated in an integrated, human-centric manner.

Exploitation Actions and Expected Return

ZORTENET's exploitation strategy is driven by the ambition to transition from a research-focused entity to a provider of advanced 5G/6G security services. The organisation has defined a clear roadmap for exploiting the HORSE results through **Internal Use (U)** to bolster its technical capacity and **Services (S)** to generate commercial value.

Concrete Exploitation Actions

ZORTENET will focus its exploitation efforts on specific project results where it has contributed to validation and integration:

- **Service-Based Commercialisation of Smart Monitoring (KER3):** ZORTENET will integrate the **Smart Monitoring** component into its existing service portfolio. Instead of a standalone product, this will be offered as a managed security service, providing telecom operators and verticals with real-time observability, anomaly detection, and data ingestion capabilities validated in HORSE.
- **Consultancy on 6G Orchestration (KER1 & ER3):** Leveraging its expertise with the **HORSE Platform (KER1)** and the **Intent-Based Interface (ER3)**, ZORTENET plans to launch a specialized consultancy service. This service will assist clients in designing secure, intent-driven network architectures, translating high-level business goals into deployable network policies using the IBI.
- **Predictive Analysis Services (KER7):** By utilizing the **Network Digital Twin (NDT)** internally, ZORTENET will offer "simulation-as-a-service" to clients. This allows for the risk-free testing of network configurations and security policies ("what-if" analysis) before deployment, a critical value proposition for high-availability sectors like transport and Industry 4.0.

Strategic Future Plans and Commitment

Looking beyond the end of HORSE, ZORTENET is committed to maintaining and evolving its contributions into a sustainable commercial portfolio. The company's post-project strategy is anchored in the **Internal Use (U)** of HORSE technologies to upgrade its R&D capabilities and the provision of serivces —including consultancy, integration, and managed security—to third parties. ZORTENET has identified specific Key Exploitable Results (KERs) and Exploitable Results (ERs) that will drive this future growth:

- **HORSE Platform (KER1):** As a contributor to the platform's integration and architecture, ZORTENET plans to leverage the full **HORSE Platform** to offer comprehensive 6G system orchestration services. By utilizing the platform internally, ZORTENET will enhance its ability to design and test complex network scenarios, offering clients a "security-by-design" orchestration framework that is 6G-ready and interoperable.
- **Smart Monitoring (KER3):** Building on its role in validating the **Smart Monitoring** component, ZORTENET will integrate these real-time observability and data ingestion capabilities into its product roadmap. This will enable the company to offer managed network monitoring services that provide deep visibility into distributed environments, supporting vertical industries in detecting and responding to anomalies faster.
- **Network Digital Twin (KER7):** ZORTENET intends to utilize the **Network Digital Twin (NDT)** environment to deliver high-value "what-if" analysis and predictive maintenance services. By simulating network states and attack scenarios, ZORTENET can provide clients with risk assessments and optimization strategies without disrupting live infrastructure.
- **Intent-Based Interface (ER3):** To simplify complex network management for its customers, ZORTENET plans to adopt the **Intent-Based Interface**. This will allow the company to offer intuitive, high-level service management solutions where user intents are automatically translated into network policies, lowering the barrier to entry for advanced 6G security operations.

Strategically, ZORTENET aims to exploit synergies between HORSE and other EU projects in which it participates (e.g., SEPTON, TRUSTEE, EVOLVED-5G), using these HORSE-derived technologies as common building blocks for trusted data spaces, secure orchestration, and Industry 4.0/6G integration. The company will actively pursue standardisation and contribution opportunities whenever HORSE outcomes mature into de-facto practices for 6G security management, and will remain engaged with the project partners to explore follow-up initiatives, pilots, and commercial deployments. By allocating internal resources for the continued development and commercialisation of these assets, ZORTENET demonstrates a clear long-term commitment to reinforcing Europe's leadership in secure, intelligent 6G infrastructures.

6.5.11 Eight Bells Ltd (8BELLS)

Partner Profile

Eight Bells Ltd (8BELLS) is an independent research and consulting firm based in Nicosia, Cyprus, specializing in selected areas of Information and Communication Technologies (ICT) as well as business modelling and analysis.

The company develops customizable solutions that support modern communications, with a strong focus on 5G mobile technologies, Network Function Virtualization (NFV), and cloud infrastructure management. 8BELLS also has extensive experience in hardware design and embedded software development, delivering a wide range of tailored solutions for contemporary IoT applications across various industries.

In the consulting domain, 8BELLS provides specialized ICT advisory services that help clients navigate dynamic market conditions and leverage new opportunities. By working closely with

its clients and employing a data-driven approach, the company delivers customized solutions aligned with specific business needs.

The team of analysts and researchers at 8BELLS has a strong R&D orientation with substantial involvement in EU- and nationally funded projects in networking and telecommunications. They have participated in numerous research initiatives and contributed to over 80 publications in international journals and conferences. The company's portfolio also includes system engineering and integration, embedded hardware and software development, network design, and innovative customized solutions.

Our technical capabilities include:

- Systems & Network Engineering: Design, implementation, and integration of communication systems and networks.
- Hardware Design: Development of microcontroller-based PCB solutions for IoT devices, supporting small or large-scale, low-cost data acquisition. Expertise includes custom sensor interfaces, signal conditioning, and various wireless sensor network protocols and topologies (WiFi, Zigbee, LoRa, etc.).
- Cloud Computing & X-as-a-Service: Design, deployment, and management of cloud infrastructures; optimized resource allocation in IaaS environments; and rapid implementation of PaaS or SaaS solutions.
- Privacy, Security & Data Protection: Cybersecurity gap assessments, virtualized cybersecurity solutions, privacy

As part of the HORSE project consortium, 8BELLS contributed in a number of distinct and meaningful ways building on its experience and competencies.

At a technical level, 8BELLS leads WP4: AI-assisted human centric Secure and Trustable Orchestration and more specifically in T4.1: Development of the Reliability, Trust and Resilience Provisioning framework and T4.4: Development of the Domain Orchestrator Connectors.

In addition, 8BELLS led the consortium-wide efforts in Exploitation (T6.4) and other similar initiatives enhancing HORSE impact. As such it has ensured that in cooperation with all project partners, HORSE's results get the exploitation support thy deserve.

Exploitation Actions and Expected Return

From the perspective of components and tools created as part of the project, 8BELLS contributed with three FG results:

- The pre-processing framework: A middleware layer for orchestrating and harmonising diverse data sources into cohesive, scalable, and analytics-ready data environments.
- The DOC: A suite of secure connectors enabling logical and physical interaction with infrastructure elements across domains.
- The RTR: A mechanism capable of generating Ansible playbooks in response to detected threats or required mitigation actions.

In terms of further exploiting the result, 8BELLS envisions a number of concrete ways that this will be made:

- Further development and validation of the above FG results and testing in real-world pilots
- Deployment in future EU projects to strengthen maturity, visibility, and validation in diverse domains.
- Expansion of the service portfolio by embedding the simulator into consulting and decision-support services offered to partners and clients.

The three FG results provided by 8BELLS can enable a broad spectrum of applications across sectors when secure orchestration, automated resilience and multi-source data harmonisation are critical. Potential target markets may be:

- Telecommunications & ICT: Cross-domain orchestration of network resources, secure connectors for multi-vendor environments, and automated mitigation playbooks for network resilience.
- Cybersecurity & Critical Infrastructure Protection: Trust and resilience provisioning, automated mitigation workflows, and infrastructure-agnostic connectors for secure system orchestration.
- Industry 4.0: Harmonisation of operational data from various sources, secure orchestration between production systems, and automated corrective actions to minimise downtime.
- Research and Innovation Community: As a foundation for next-generation orchestration frameworks and resilience-by-design systems deployed in EU-funded pilots and testbeds.

Building upon the maturity achieved within HORSE, 8BELLS identifies several pathways to further exploit and advance the three FG results:

- Go-to-Market Strategy: Promote the Pre-processing, DOC, and RTR components as modular solutions that can be adopted individually or as part of an integrated orchestration package.
- Partnership Development: Engage with technology providers, infrastructure operators, and cybersecurity vendors to validate the components in real operational environments
- EU Projects & Innovation Networks: Leverage forthcoming R&I initiatives as opportunities to increase the TRL of the components.

8BELLS anticipates several types of returns arising from the exploitation of the Pre-processing, DOC, and RTR results:

- Economic returns: New revenue streams from licensing, consultancy services, integration work, and potential SaaS-based delivery of the orchestration and resilience components.
- Strategic returns: Strengthening 8BELLS' position in the telecommunications and network security markets and broadening the company's portfolio
- Knowledge-based returns: Enhanced expertise in middleware-based data harmonisation (Pre-processing), secure cross-domain connectivity (DOC), and automated resilience provisioning (RTR).

Strategic Future Plans and Commitment

As a technology-oriented SME with a strong focus on cybersecurity, 8BELLS intends to further capitalise on the FG results generated within HORSE. The company has a strong interest in advancing trustworthy automation and resilience technologies aligned with real-world applications.

Recognising the significant potential of the above components as well as KER5 - Intent-based Secure cross-Domain Orchestrator, 8BELLS plans to continue their development, validation, and adaptation in order to integrate them into its broader service and solution portfolio. Priority will be given to maturing the components through upcoming R&I initiatives, real-world pilot deployments, participation in dissemination events and collaborations with industrial actors.

Furthermore, 8BELLS is committed to maintaining and building upon the strong collaborations established within HORSE. Partners involved in the project represent valuable stakeholders for future joint activities, including follow-up R&I proposals, technology integration efforts, and business-oriented engagements.

6.5.12 Martel Gmbh (MAR)

Partner Profile

Martel Innovate is a dynamic digital innovation consultancy company specialising in ICT research and development. Its core R&D activities focus on cloud and edge computing, the Internet of Things, artificial intelligence, mobile communications, and open-source software engineering. In addition to its research expertise, Martel offers an IoT platform and a wide array of communication, marketing, media, and training services. With over two decades of experience in European Commission R&D programmes and a strong track record in delivering innovation projects, Martel has established a solid presence in the Swiss and Dutch markets, consistently turning research ideas into practical, valuable products.

Exploitation Actions and Expected Return

Martel has made a plan to integrate HORSE technology for enhancing its IoT platform, Orchestra Cities, as part of its commercial expansion into the Swiss market. Specifically, Martel plans to adopt several architectural designs and software components developed by the HORSE project to modernise the platform:

- Common Knowledge Base (cKB): Developed by Martel, this database is crucial for gathering and sharing threat intelligence in HORSE. CKB is an AI-augmented knowledge base for attack classification and mitigation strategies, mapping attacks to countermeasures.
- Attack/Mitigation Service: Also developed by Martel, this service is designed to offer a high-level interface to cKB. Clients query the service to obtain mitigation strategies for specific attacks.
- Ansible Playbooks: developed by other HORSE partners, these playbooks operationalise attack mitigation strategies.
- Know-how: valuable technical knowledge of AI and threat intelligence, acquired during the implementation of HORSE and essential for ongoing development, refinement processes, and future research within the SNS program.

Presently, Orchestra Cities lacks a threat intelligence solution. The platform needs the means to bridge the gap between attack detection and response. KB, Attack/Mitigation Service, and Ansible Playbooks will bridge this gap, allowing system administrators to swiftly respond to attacks with a semi-automated procedure where suitable mitigation strategies are suggested, validated, and then implemented by running playbooks.

By integrating HORSE technology, Orchestra Cities will evolve from a purely IoT platform into an intelligent, security-aware IoT management environment. This will enable:

- Rapid incident response via semi-automated mitigation workflows.
- Reduced downtime and improved cyberattack resilience for smart city infrastructure.
- Differentiation in the competitive IoT platform market by embedding AI-driven cybersecurity intelligence.

Target customers include Swiss municipalities and utilities, as well as European smart city operators seeking GDPR-compliant, secure IoT platforms.

The integration of HORSE threat intelligence into Orchestra Cities is expected to contribute ~5–10% of total Orchestra Cities revenue by year 2 post-project.

Strategic Future Plans and Commitment

Martel is fully committed to sustaining and further developing the results achieved through the HORSE project beyond its lifetime. Building upon the project's technological assets, Martel's strategic ambition is to transform Orchestra Cities into a up-to-date sustainable, and security-aware IoT platform that supports the next generation of intelligent, trustworthy, and interoperable digital infrastructure.

Product Integration and Commercialisation

The HORSE-derived components (KB, Attack/Mitigation Service, Playbooks) will be integrated into the current Orchestra Cities platform as part of a new Advanced Security Suite. This suite will be offered to customers as a modular, premium add-on, enabling data-driven threat detection and semi-automated incident response. The solution will be maintained and updated regularly to incorporate the latest threat intelligence, ensuring long-term technological relevance and customer trust.

Service Model and Continuous Value Creation

Martel will introduce a subscription-based service offering that includes configuration support, threat intelligence updates, and maintenance. This model ensures a sustainable revenue stream while providing customers with continuous protection improvements and technical assistance. Lessons learned during early deployments will be fed back into R&D activities to further enhance system resilience and automation capabilities.

Market Expansion

In the first phase, the enhanced Orchestra Cities platform will be piloted with existing Swiss customers—primarily municipalities and utilities. In a second phase, Martel plans to expand to wider European markets through cloud-based deployments and strategic partnerships with smart city operators and cybersecurity providers. Engagement in relevant European initiatives and standardisation groups (e.g., NGIoT or ETSI) will reinforce interoperability and increase visibility among public sector and industrial stakeholders.

Sustainability and Commitment to the EU Digital Agenda

This exploitation strategy is fully aligned with Horizon Europe's objectives on digital resilience, open innovation, and secure data ecosystems. Martel's long-term commitment includes continued investment in R&D for AI-driven cybersecurity, participation in future European collaborative projects, and contribution to open-source communities. By leveraging HORSE results, Martel aims to strengthen Europe's capacity for secure and trustworthy digital transformation.

6.5.13 Sphynx Technology Solutions AG (STS)

Partner Profile

Sphynx Technology Solutions AG (STS) is a cybersecurity technology and innovation company specialising in advanced cyber risk management. With a strong R&D presence across Switzerland, Greece, and Cyprus, STS develops next-generation platforms for Security Operations, Threat Intelligence, and Assurance, bridging research with practical enterprise solutions.

STS is recognised for its Security and Privacy Assurance (SPA) platform, combining analytics, AI-driven threat detection, and much more. The company actively participates in multiple European research initiatives focused on AI-enabled cybersecurity, privacy assurance, and digital trust frameworks.

Within HORSE, STS contributes core expertise in cybersecurity observability and compliance orchestration, leading the design and development of the Smart Monitoring (SM) and Compliance Assessment (CAS) components under Work Package 4). These modules provide the backbone for secure data collection, policy validation, and compliance assurance in 6G network environments.

Through these contributions, STS reinforces HORSE's mission to deliver a resilient, trustworthy, and autonomous 6G security platform that integrates real-time monitoring, policy enforcement, and AI-based reasoning.

Exploitation Actions and Expected Return

Relevant HORSE results/components

- **Smart Monitoring (SM):** real-time observability and data ingestion framework integrating Elastic-based pipelines for data distribution.
- **Compliance Assessment System (CAS):** Open Policy Agent (OPA)-based compliance engine that validates orchestrated actions against regulatory, operational, and ethical policies (GDPR, NIS2, DORA).

Target markets and domains

- Telecommunications operators and managed service providers deploying secure 5G/6G networks.
- Financial, healthcare, and energy sectors adopting compliance-driven security orchestration.
- Public administration and critical-infrastructure operators requiring automated regulatory assurance.

Exploitation scenarios

- Integration of HORSE's SM and CAS components into STS's commercial SPA Suite and SOAR Platform, expanding their functionality toward real-time network compliance monitoring.
- Participation in follow-up SNS JU or Digital Europe initiatives, reusing HORSE software assets as building blocks for new cybersecurity demonstrators.

Expected returns

- **Economic:** creation of new service offerings and licensing opportunities for the HORSE-derived modules.
- **Strategic:** strengthened position in the European 6G cybersecurity ecosystem as a provider of orchestration technologies.
- **Knowledge-based:** enhanced capabilities in cloud-native monitoring, policy-driven orchestration, and federated compliance analytics.
- **Policy/standardisation:** contribution to the evolution of EU compliance automation frameworks and alignment with ETSI/NIS2 implementation guidelines.

Strategic Future Plans and Commitment

STS plans to sustain and expand HORSE outcomes by embedding the Smart Monitoring and Compliance Assessment technologies into its commercial and R&D portfolio.

Post-project actions include:

- **Product integration:** full incorporation of HORSE-derived observability and compliance modules into the SPA Suite and SOAR platform, enabling continuous regulatory assurance for 5G/6G operators.

- **Service expansion:** deployment of HORSE-based capabilities in STS's Cyber Range for training, simulation, and compliance validation.
- **Investment commitment:** dedicated engineering and compliance teams to maintain and evolve HORSE components within STS's product roadmap.
- **Strategic alignment:** HORSE directly supports STS's mission to drive digital trust and security automation as core pillars of Europe's Industry and digital-sovereignty agenda.

By extending HORSE technologies into its operational platforms and service offerings, STS aims to deliver measurable impact, advancing the automation, transparency, and trustworthiness of cybersecurity operations across European digital infrastructures.

6.5.14 Universidad de Murcia (UMU)

Partner Profile

The University of Murcia (UMU) is a public academic and research institution with strong expertise in 5G technologies, network orchestration, policy-based management, and infrastructure deployment. UMU has extensive experience in designing and managing experimental testbeds, integrating cloud and edge components, and supporting research on secure and automated network control mechanisms.

UMU has contributed by providing the UMU testbed, which offers the experimental infrastructure required to deploy and validate the different components of the platform under realistic conditions, in addition to the proposed 5G infrastructure. Additionally, UMU has developed/integrated two complementary software components that interact with the HORSE ecosystem: the Bastion security orchestrator, responsible for enforcing security policies both over the real infrastructure and within the Impact Analysis Digital Twin (IA-NDT), and the Policy Translator, which acts as a proxy and translator between the IBI/EM and UMU orchestrator.

Exploitation Actions and Expected Return

As an academic and research institution, the University of Murcia (UMU) focuses its exploitation strategy primarily on scientific and academic impact, reinforcing its expertise in 5G technologies, orchestration, and policy-based network management. Within the HORSE project, UMU's most relevant contributions are the Bastion Orchestrator, a background component (BG) responsible for enforcing security policies across both the real infrastructure and the Impact Analysis Digital Twin (IA-NDT), and the Policy Translator, which facilitates the interaction between the IBI/EM and the orchestration layer through an automated translation process.

The Bastion Orchestrator constitutes a key technological outcome that will be further developed and integrated in future research initiatives and collaborative projects. Although not released as open-source, the framework can be shared under permission agreements, enabling its use in experimental or applied research contexts where automated policy enforcement and orchestration are required. Similarly, the UMU testbed will remain a valuable asset for validating core 5G environments and for generating realistic user-plane and data-plane traffic in forthcoming research activities.

UMU's exploitation actions are thus oriented toward academic dissemination, collaborative research, and knowledge transfer, ensuring that the results achieved in HORSE strengthen its research group's capacity to address challenges in 5G/6G orchestration, security automation, and digital twin validation.

The expected returns are mainly knowledge-based and strategic. On the one hand, the experience gained through the development and integration of Bastion and the Policy

Translator enhances UMU's scientific and technical capabilities in secure orchestration and infrastructure automation. On the other hand, these advancements reinforce the institution's positioning in the European research landscape, providing potential influence in future directions related to 6G security orchestration and policy-driven network management, and laying the groundwork for participation in new collaborative projects and standardisation discussions.

Strategic Future Plans and Commitment

UMU plans to sustain and extend the impact of HORSE primarily through academic exploitation and research-driven innovation. The results will be integrated into Master's theses and Ph.D. projects, ensuring that the knowledge and technologies developed continue to foster training, experimentation, and the development of next-generation orchestration and security mechanisms.

In the medium to long term, UMU remains open to further collaboration with HORSE partners in future research proposals, standardisation efforts, or joint activities that align with the project's technological domains. These future actions are consistent with UMU's broader strategic objectives in digital transformation and Industry 5.0, reinforcing its commitment to advancing secure, intelligent, and automated network infrastructures.

6.6 HORSE Contributions to EU Sustainable Development Goals as part of the UN 2030 Agenda for Sustainable Development

The United Nations' 2030 Agenda for Sustainable Development [5] presents a comprehensive framework designed to foster a more inclusive and sustainable future worldwide. At the core of this agenda are the 17 Sustainable Development Goals (SDGs), which seek to tackle major global challenges, including poverty, inequality, climate change, environmental degradation, as well as issues related to peace and justice.

The HORSE project can contribute to two of the SDGs, namely **SDG 9: Industry, Innovation and Infrastructure** and **SDG 11: Sustainable Cities and Communities**.

In relation to SDG 9, HORSE aligns with the UN's objective of building resilient infrastructure and fostering innovation by addressing the growing cybersecurity challenges associated with next-generation communication networks. As 5G and 6G services become the backbone of critical infrastructures, industrial systems, smart cities, and global connectivity, ensuring their security and reliability is increasingly vital. Cyber threats pose significant risks to network availability, data integrity, and service continuity, potentially undermining economic activities and technological progress. HORSE responds to these challenges by providing intelligent, AI-driven cybersecurity mechanisms capable of detecting, preventing, and mitigating cyberattacks in real time.

HORSE can also contribute to SDG 11, which focuses on making cities and human settlements inclusive, safe, resilient, and sustainable. The deployment of 5G and future 6G networks is a key enabler of smart city applications, such as intelligent transportation systems, smart energy grids, environmental monitoring, and IoT-enabled public services. These technologies allow cities to optimize resource usage, reduce emissions, improve service efficiency, and enhance quality of life for citizens. However, the increasing interconnection of urban infrastructures also expands the attack surface, making robust cybersecurity a prerequisite for sustainable smart city development. HORSE addresses this need by ensuring secure data transmission, protecting IoT devices and critical urban services, and enabling continuous monitoring and rapid response to cyber threats.

7 Standardisation

Since its initial stages, HORSE aimed to integrate its outcomes into industry standards to ensure global adoption of the technologies developed and validated within the project. Being aware of the need for timely standardization actions to achieve industry uptake, the project actively monitored relevant communities of any nature (SDOs as such, industry fora, open-source communities…), adapting its contribution approach to maximize impact, and aiming at enhance influence by addressing leadership positions and by shaping the creation of specific groups and the definition of work-items within them.

As reported in D6.2, during the first phase of the project 50 contributions were recorded in the standards contribution tracker, classified according to the categories identified in that document. At the moment of the writing of this deliverable, 122 additional contributions have been reported in the tracker, and classified according with the same categories. In both periods, the main standardization targets were IETF and ETSI, together with specific actions and collaborations focused on 3GPP, as the main source for future 6G specifications, and OSM, as reference open-source community.

7.1 IETF

A significant part of the activity during this period has focused on the Internet Engineering Task Force (IETF), where HORSE partners, led by TID, contributed to multiple working groups, especially in the Operations and Security areas. These working groups include OPSAWG, IVY, NMOP, NETCONF, NMRG and RATS, alongside emerging initiatives such as WIMSE and NSAR. Key milestones included the progress of the initiatives related to NDT architecture and intent modelling, the adoption of relevant aspects for telemetry data such as YANG data provenance, data manifests and configuration tracing, and the entitlement and capability models for network inventory management.

Beyond document contributions, HORSE actively participated in IETF hackathons, demonstrating practical implementations of its proposals, focused on telemetry data and the use of semantic models for NDT definition and management. These demonstrations were intended to demonstrate the technical feasibility of the proposals and to accelerate the path towards standardization by addressing the IETF motto of *rough consensus and running code*.

7.2 ETSI

The project has contributed to several technical committees and industry specification groups within ETSI, addressing practically all technical groups related to security, AI and network management, with contributions to TC DATA, ISG ZSM, TC CYBER, TC SAI, ISG ENI, etc. It is worth noting the leadership positions in ISG ZSM and the process for creating and leading TC DATA.

The leadership within ETSI ZSM has facilitated, as a natural evolution of this group focused on network automation, to a discussion on how the activities related to network technologies should evolve in ETSI. Beyond this, this leadership position has also allowed us for driving discussions on NDT applicability, interfaces and architectural requirements, intent-based closed-loop management, trust frameworks, and the evolution toward autonomous networks. The project also delivered a comprehensive Proof of Concept (PoC), ZSM PoC#15 [6], demonstrating the use of the two Network Digital Twins (NDTs) developed by the project, and illustrating how these two NDTs cooperate as part of a sandbox environment, working together to mitigate cyberattacks, supporting minimally invasive smart automated threat management. This PoC was demonstrated at the ZSM#33 plenary meeting, and a final report on it is being prepared, and will be made available at the PoC page in ETSI, as shown above.

TC DATA is the new technical committee dedicated to data solutions, committed to address issues regarding European regulation on data and data-enabled ICT services, such as the Data Act and the AI Act. HORSE partners played a key role in the inception of the technical committee, assumed leadership roles and shaped the initial work program. This committee is introducing multiple new work items on topics such as data governance, smart contracts, data quality metrics and data ontologies for their use by AI components, all of which align closely with HORSE exploitation objectives beyond the project span.

7.2.1 ETSI ZSM PoC

The project also delivered a comprehensive Proof of Concept (PoC), ZSM PoC#15 [6], demonstrating the use of the two NDTs developed by the project, and illustrating how these two NDTs cooperate as part of a sandbox environment, working together to mitigate cyberattacks, supporting minimally invasive smart automated threat management. This PoC was demonstrated at the ZSM#33 plenary meeting in Granada, and a final report on it has been submitted, and it is available at the PoC page in ETSI, as shown above.

7.3 Other Bodies and summary of the contributions

HORSE kept its activity within 3GPP, focused on SA3 (security) and SA5 (operations and management), contributing to the definition of security aspects for future 6G-related releases and influencing discussions on application of AI and NDT technologies. Some project viewpoints were explicitly referenced during the 3GPP 6G Workshop, including recommendations on AI-driven intent management.

Additionally, the project engaged with the OSM open-source community, addressing their long-term view and making contributions on NDT orchestration.

As a summary of all the standardisation activities that has been carried out in the last year of the project, the final snapshot of the tracking tool is presented in Appendix G – Final standardisation activities.

8 Conclusions

The Final Impact Creation Report and Exploitation Plan (D6.3) consolidates the project's achievements from a strategic perspective, highlighting how technical innovation has been complemented by structured dissemination, collaboration, and exploitation activities. The extensive communication and dissemination actions carried out throughout the project have ensured strong visibility within the scientific, industrial, and standardisation communities, while fostering meaningful synergies with related initiatives in the SNS ecosystem.

A key outcome of the project is the clear identification and management of intellectual property, resulting in a well-defined portfolio of BG and FG assets, ERs and KERs. The exploitation strategies presented in this report demonstrate a balanced approach, supporting further research, industrial uptake, commercialisation, and standardisation-driven impact.

Moreover, HORSE's engagement with the Horizon Results Booster programme and its contributions to standardisation bodies and EU sustainability objectives underline the project's commitment to responsible innovation and long-term value creation.

9 References

[1] “Europe - IP Glossary - I - IP Helpdesk - European Commission.” Accessed: Dec. 30, 2025. [Online]. Available: https://intellectual-property-helpdesk.ec.europa.eu/regional-helpdesks/european-ip-helpdesk/europe-glossary/europe-ip-glossary-i_en

[2] “IP guides - IP Helpdesk - European Commission.” Accessed: Dec. 30, 2025. [Online]. Available: https://intellectual-property-helpdesk.ec.europa.eu/regional-helpdesks/european-ip-helpdesk/ip-guides_en

[3] “Dissemination and exploitation of research results - Research and innovation.” Accessed: Dec. 30, 2025. [Online]. Available: https://research-and-innovation.ec.europa.eu/strategy/dissemination-and-exploitation-research-results_en

[4] “About,” Booster. Accessed: Dec. 30, 2025. [Online]. Available: https://www.horizonresultsbooster.eu/about

[5] “THE 17 GOALS | Sustainable Development.” Accessed: Dec. 30, 2025. [Online]. Available: https://sdgs.un.org/goals

[6] “PoC 15 Trustworthy Zero-touch Network and Service Management in 6G Networks with NDT support - ZSM Wiki.” Accessed: Dec. 30, 2025. [Online]. Available: https://zsmwiki.etsi.org/index.php?title=PoC_15_Trustworthy_Zero-touch_Network_and_Service_Management_in_6G_Networks_with_NDT_support

10 Appendix A – HORSE latest newsletter

View in browser

Welcome to the 4th edition of the HORSE project newsletter. HORSE: Holistic, Omnipresent, Resilient Services for Future 6G for Wireless and Computing Ecosystems, proposes a novel human-centric, open-source, green, sustainable, coordinated provisioning and protection evolutionary platform, which can inclusively yet seamlessly combine advancements in several domains.

Read here about news, analyses, visionary articles from the 5G/6G and digital technologies and events update from the HORSE project community.

LATEST NEWS

2nd IEEE Workshop on "The Path Towards 6G: Standardization and Research Vision" – Paper submission deadline

Key innovations in cybersecurity and privacy in the European 6G ecosystem

HORSE Key Achievement: What-If

HORSE Key Achievement: Attack and prediction modelling

HORSE Key Achievement: ML Detector Engine

HORSE Contributions

WHITE PAPER: European Vision for the 6G Network Ecosystem
This white paper focuses on the ongoing global efforts to develop and standardise 6G networks, aiming for a commercial launch around 2030.

WHITE PAPER: AI Technologies in Experiential Networked Intelligence to Increase Autonomous Operation
ISG ENI focuses on defining the functionalities and architecture to increase the Autonomous operation of a communication network, thereby enhancing the overall operator experience.

FOLLOW US

www.horse-6g.eu

Co-funded by the European Union

6GSNS

HORSE project has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101096342. This work has received funding from the Swiss State Secretariat for Education, Research and Innovation (SERI).

HORSE project

Newsletter managed by Martel GmbH

111 Überlandstrasse,
8600 Dübendorf
Switzerland

horse-6g.eu

You have received this email because you provided consent to receive a newsletter with updates about our project via a service powered by HORSE, such as the project website or project events.

Unsubscribe

11 Appendix B – Module A templates

KER1 – HORSE platform

Exploitation intentions table for KER1 - HORSE Platform	
Description	This KER represents the entire HORSE architecture. The architecture is intended to be deployed on top of 5G/6G infrastructures.
Target market/ end users	The HORSE architecture can be intended as a product to increase the readiness to security issues and threats to services and the communication infrastructure. It can be deployed on top of existing infrastructure, and it provides an autonomous process for detection and mitigation of security threats. Target market can be Telcos, virtual mobile network operators and OTT and service providers.
Competitive advantages	Competitive advantages: Fully distributed, fully modular, prediction of security scenarios, capable of identifying the most appropriate mitigation action, intent-based strategy for security management. To the best of our knowledge, most of current solutions address specific aspects only (e.g. firewall, IDS, anti-virus), while this KER enables policy-based control and automated reaction to security threats.
Use model	Currently, the KER is put to use for publications, contributions/PoC to standardization bodies, teaching and further development in future research initiatives. Beyond that technology transfer, service provision and licensing may be seen as potential strategies to put HORSE into use. Moreover, the two use cases proposed in the project for validation purposes, may be considered as early adopters of the proposed solution, one in the transportation sector and another one in the media/entertainment. It is yet to be defined what might be the proper model to spread out the HORSE solution to the potential users.
Partners	CNIT (owner, leader for further R&D and exploitation activities), UPC (owner, leader for further R&D activities), the rest of the consortium partners will support the above activities and have equal ownership percentage.
Timing	This KER is a complete architecture. Therefore, it is difficult to estimate the time to market. The concept/architectural framework is ready to be integrated, while a complete deployment of the entire system requires further engineering. A very rough estimation can be in 3-5 years after the project end.
IP status	Since this KER involves all consortium members, the IPR strategy will be discussed and finalised in the future always in line with GA and CA.

KER2 - Distributed AI Engine for Services Preassesment

Exploitation intentions table for KER2 - Distributed AI Engine for Services Preassesment	
Description	The Distributed AI Engine for Services Preassesment aims to effectively engage the minimum number of available resources in a 6G network for proper service execution. It relies on proper model training in a federated fashion way by taking into consideration various performance metrics, such as service complexity, hardware resources, security policies, etc.
Target market/ end users	The target market mainly refers to Network and application providers and especially 6G network providers or other beneficiaries who make use of 6G resources, e.g. smart grid market users. 6G network users or smart electrical grid users.
Competitive advantages	Optimum resource allocation in complex environments, such as the 6G framework, which are based on the integration of various heterogeneous resources, Distributed AI/ML models that analyze a vast amount of data and identify issues that prevent optimum service deployment.
Use model	Service of the KER will be provided on an open-source basis.
Partners	NKUA (owner, leader for further R&D and exploitation)
Timing	1-2 years after the project completion
IP status	The IPR mechanism that will be used to protect this KER will be Copyright and will be formally registered in the future. The entire IPR strategy will be in line with GA and CA.

KER3 – Smart Monitoring (SM)

Exploitation intentions table for KER3 - Smart Monitoring (SM)	
Description	Smart Monitoring is a data collection and analysis component designed to provide real-time insights into operational and security states within high-performance, next-generation networks, particularly 6G. It collects, processes, and stores diverse data types (e.g., network traffic, analytics, device identifiers) and exposes this information through secure APIs and visualization dashboards. Smart Monitoring is the core observability and data backbone of the HORSE platform, enabling robust, scalable, and secure data ingestion and distribution.
Target market/ end users	Target market: High-performance telecom environments, particularly for 6G networks and advanced research testbeds. Potential end-users: Cybersecurity vendors, telecom operators, infrastructure vendors, cybersecurity researchers.
Competitive advantages	Smart Monitoring is purpose-built for high-intensity 6G environments, offering reliable monitoring across diverse data types like pcap, analytics, and device identifiers. Unlike generic tools, it is deeply integrated into the HORSE platform (as will be in our platform as well), ensuring compatibility with specific system needs and high-volume data flows. Smart Monitoring intelligently adapts to complex, high-volume environments and it turns raw data into actionable knowledge (securely, flexibly, and in real time).
Use model	SM will be a part of other STS systems and components.
Partners	STS (owner, leader for further R&D and exploitation)
Timing	1-2 years after the project completion
IP status	The IPR mechanism that will be used to protect this KER will be Copyright and will be formally registered in the future. The entire IPR strategy will be in line with GA and CA.

KER4 – Threat detector and mitigation engine

Exploitation intentions table for KER4 - Threat detector and mitigation engine (DEME)	
Description	KER4 is a software artifact that leverages Machine Learning algorithms, combined in an innovative way, to detect network attacks and subsequently trigger mitigation actions.
Target market/ end users	Ericsson retains intellectual property rights over its implementations within research projects, as these types of innovative modules can be integrated into Ericsson products, particularly within the OSS domain and specifically in Network Management Devices or SIEM systems. The OSS clearly represents the "brain" of Ericsson's network solutions, and as such, every evolutionary enhancement or new feature can provide a competitive advantage. This added value can positively differentiate Ericsson in the eyes of its clients—typically the world's largest telecom providers—especially in an increasingly competitive and challenging market.
Competitive advantages	The threat detector developed within the HORSE project introduces an innovative architectural concept specifically designed to more effectively address new or zero-day attacks. These types of threats are expected to increase significantly in the context of 6G, and current systems are not yet adequately prepared to handle them.
Use model	Ericsson employs a Toolgate process, an enhanced variant of the traditional Phase-Gate model, which not only guides product development but also steers business model validation and project management decisions. At each step, the process integrates structured evaluation tools to assess technical progress, market fit, and strategic alignment. Based on the outcomes, dedicated checkpoints trigger decision phases on resource allocation and business direction—for example, accelerating efforts to seize a market window or discontinuing activities that no longer meet expectations. Early customers are selected among Ericsson's most loyal telecom provider partners, who gain early access to innovative solutions and contribute valuable feedback during piloting.
Partners	ETI (owner, leader for further R&D and exploitation)
Timing	Innovative features that can provide a competitive advantage should be introduced as early as possible. However, their preliminary assessment must be thorough, involving in-depth technical evaluations and well-structured decision-making phases. These phases cannot be compressed or bypassed, as doing so would increase the risk of misjudgements or poor investment decisions. For this reason, now that the implementation and integration of the component have been completed, it is essential to dedicate the remaining six months of the project to an intensive performance testing and validation campaign.

IP status	There is certainly an IP strategy in place, and it plays a crucial role. The Consortium Agreement specifically outlines the clauses regarding the use of solutions conceived and developed by individual partners—in this case, Ericsson—and serves as the legal reference framework governing intellectual property rights.

KER5 – Intent-Based Secure cross-Domain Orchestrator

Exploitation intentions table for KER5 - Intent-Based Secure cross-Domain Orchestrator	
Description	Includes a set of tools to logically and physically interact with the infrastructure elements to provide a secure cross domain orchestration. The interaction will be handled through a proper mapping of high-level intents into security workflows able to react to security threats and vulnerabilities.
Target market/ end users	Target Market: The global cybersecurity and network orchestration market, particularly in 5G/6G telecommunications, cloud computing, and multi-stakeholder infrastructure management. Potential end-users: Telecommunication operators, cloud service providers and enterprise IT departments requiring secure, scalable orchestration across distributed networks. Early adopters include major telecom providers and large-scale cloud operators seeking to enhance security and efficiency.
Competitive advantages	The Intent-Based Secure Cross-Domain Orchestrator offers superior solutions by: - Integrating advanced NLP and LLMs in the KB for dynamic threat-mitigation pairing, outpacing traditional rule-based systems. - Providing a modular DOC design that adapts to diverse network segments, surpassing rigid, segment-specific solutions. - Enabling rapid, automated threat response through RTR's structured command generation, offering a significant edge over manual or slower competitor solutions.
Use model	The KER will be further exploited through: - Service Provision: Offering managed security orchestration services to enterprises possibly via a subscription model.
Partners	8BELLS (owner, leader for further R&D and exploitation)
Timing	1-2 years after the project completion

IP status	The IPR mechanism that will be used to protect this KER will be Copyright and will be formally registered in the future. The entire IPR strategy will be in line with GA and CA.

KER 6 - End to end Proactive Secure Connectivity Manager (ePEM)

Exploitation intentions table for KER 6 - End to end Proactive Secure Connectivity Manager (ePEM)	
Description	The End-to-end Proactive Secure Connectivity Manager (ePEM) is a Key Exploitable Result (KER6) within the HORSE project. It involves a set of tools designed to logically and physically interact with infrastructure elements to provide a secure cross-domain orchestration. This interaction is handled through a proper mapping of high-level intents into security workflows capable of reacting to security threats and vulnerabilities. More specifically, this component, also known as the ePEM, oversees service orchestration. It supports the recursive deployment of many functional components for multi-tenancy and high device heterogeneity through virtualization. Crucially, it enables end-to-end resource self-configuration and the provision of a secure framework that can span across multiple domains and applications. As an Operations Support System (OSS) module, it is based on the Open-Source MANO orchestrator and is capable of orchestrating requests from the Platform Intelligence (PIL) module to the available infrastructure domain. The ePEM manages functions and operations for the placement of PIL modules, services, and applications over the available infrastructure, and for their connection to a properly configured network slice. It also maintains information about deployed applications, network services, and available infrastructure resources. The software is designed with a highly modular architecture, utilizing state-of-the-art cloud-native stateless services (with state maintained in external databases like MongoDB and Prometheus) for inherent parallelization. Its sub-modules include proactive load balancing, an Authentication Manager supporting inter-domain and edge authentication, and a Slicing Manager for adding slice-specific virtualized network functions to ensure predefined security levels per service slice. It interfaces proactively with the PIL component through the Reliability, Trust and Resilience Provisioning (RTR) module.
Target market/ end users	The Secure e2e connectivity Manager is aimed at stakeholders who manage complex, multi-domain 6G networks. Key target markets and end-users include: • Mobile Network Operators (MNOs) and telecommunication companies. • ICT vendors/providers and Software developers. • Cloud providers

	• Vertical industries as users, particularly those benefiting from multi-tenancy models and secure, host-neutral infrastructure. • Multiple infrastructure providers who are involved in the deployment, hosting, and orchestration of network services in host-neutral model. SMEs and innovators who can further develop applications, new business models, and innovative services on top of HORSE technologies.
Competitive advantages	• It provides a secure framework that spans across multiple domains and applications, addressing the complex security challenges of disaggregated, virtualized, and multi-vendor 6G infrastructures. • It implements an AI-assisted secure and trustable orchestration component that proactively and reactively enhances end-to-end network security. This includes techniques like logical VNF and traffic separation, DLT-based cross-domain trusting mechanisms, and network slice isolation. • Being based on the Open-Source MANO orchestrator and designed with a highly modular, cloud-native architecture, it promotes flexibility, scalability, and avoids vendor lock-in. • It incorporates proactive load balancing and advanced Authentication and Mobility Management capabilities supporting inter-domain and edge authentication, ensuring adaptive and dynamic security. • It enables the sharing of existing 5G and new 6G infrastructure by many operators in a multi-tenant environment, which can lead to new business models and reduced complexity and costs (CAPEX/OPEX). • It contributes to the security of host-neutral 6G primary infrastructure. It ensures secure, privacy-preserving, and trustworthy services for multi-stakeholder environments.
Use model	Now, the KER is used for teaching, publications, projects, and contributions to standards/PoCs. Early adopters are mostly researchers in the field of computer networks or mobile networks. In addition, the Secure e2e connectivity Manager functions as an Operations Support System (OSS) that effectively manages and coordinates heterogeneous resources across diverse domains.
Partners	CNIT (owner, leader for further R&D and exploitation)
Timing	1-2 years after the project completion
IP status	The IPR mechanism that will be used to protect this KER will be Copyright and will be formally registered in the future. The entire IPR strategy will be in line with GA and CA.

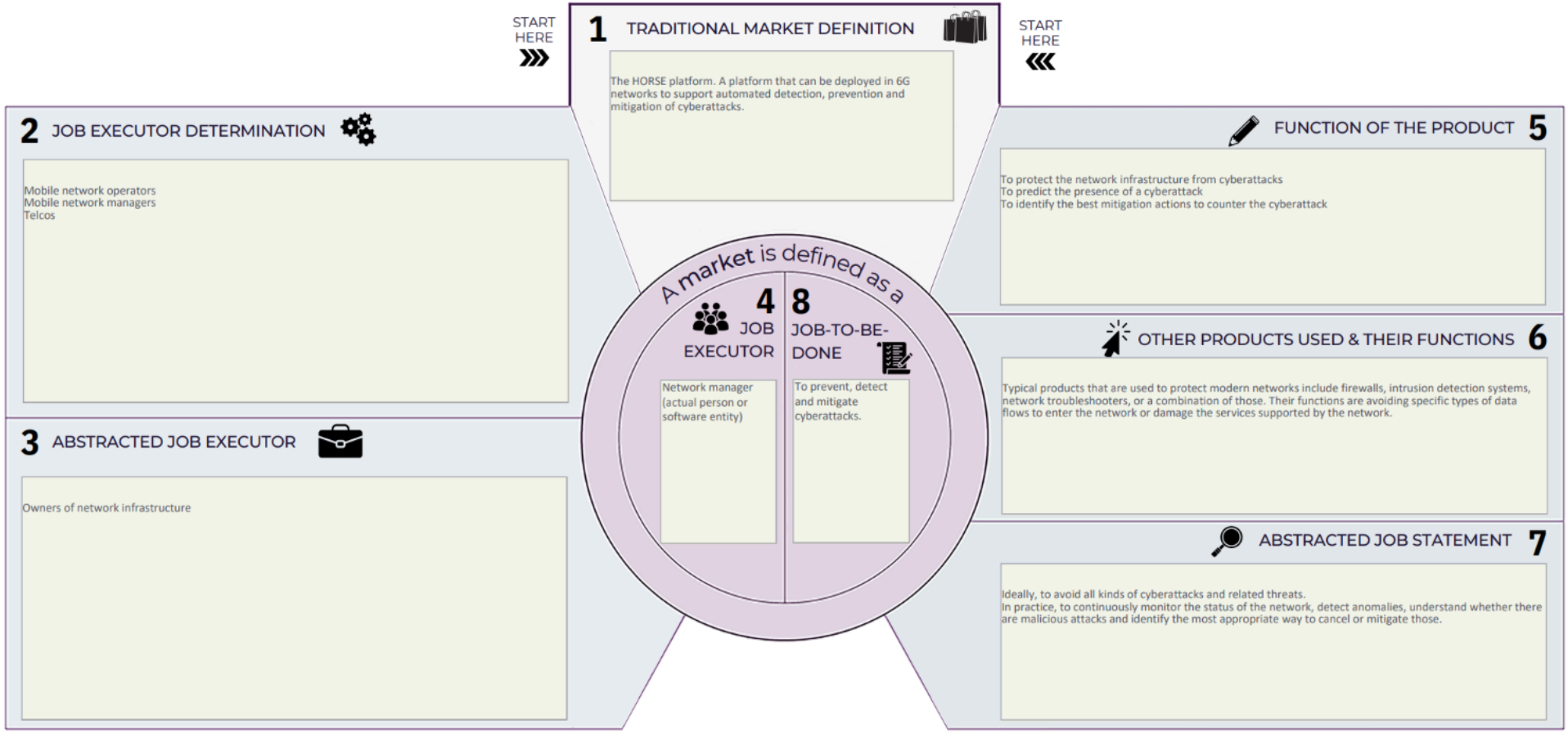
KER 7 - Network Digital Twin

Exploitation intentions table for KER 7 - Network Digital Twin	
Description	The Network Digital Twin is a replica of the real network infrastructure. It is implemented in a sandbox as a Virtual Machine or a set of containers managed by a Kubernetes environment. The Network Digital Twin replicates with accuracy the status and behaviour of the Physical Twin (e.g. the original network infrastructure).
Target market/ end users	The KER represents a module of a network management system that can be used for (i) prediction of security attacks and anomalies, and (ii) analysis of the impact of potential mitigation actions in a sandbox before implementing those on the actual infrastructure. Target market includes: mobile networks and cybersecurity, telcos, virtual mobile network operators. Potential end users can be: Network managers, system integrators in Infrastructure providers, software engineers in Service providers.
Competitive advantages	Very few Network Digital Twins are available in the market. The NDTs developed in HORSE are targeted especially to 5G/6G mobile networks. They accurately replicate most functions of the actual mobile networks by using open-source implementations of 5G. The KER is being tested on different testbeds, showing good portability. Very few NDTs are capable of real time synchronization with the actual Physical Twin, therefore this KER can be used to real time operation and prediction of events.
Use model	At the moment, the KER is used for teaching, publications, contribution to standards/PoC. Early adopters are mostly researchers in the field of computer networks or mobile networks.
Partners	CNIT and TID (owners, leaders for further R&D and exploitation activities)
Timing	1-2 years after the project completion
IP status	The IPR mechanism that will be used to protect this KER will be Copyright and will be formally registered in the future. The entire IPR strategy will be in line with GA and CA.

12 Appendix C – Module B templates

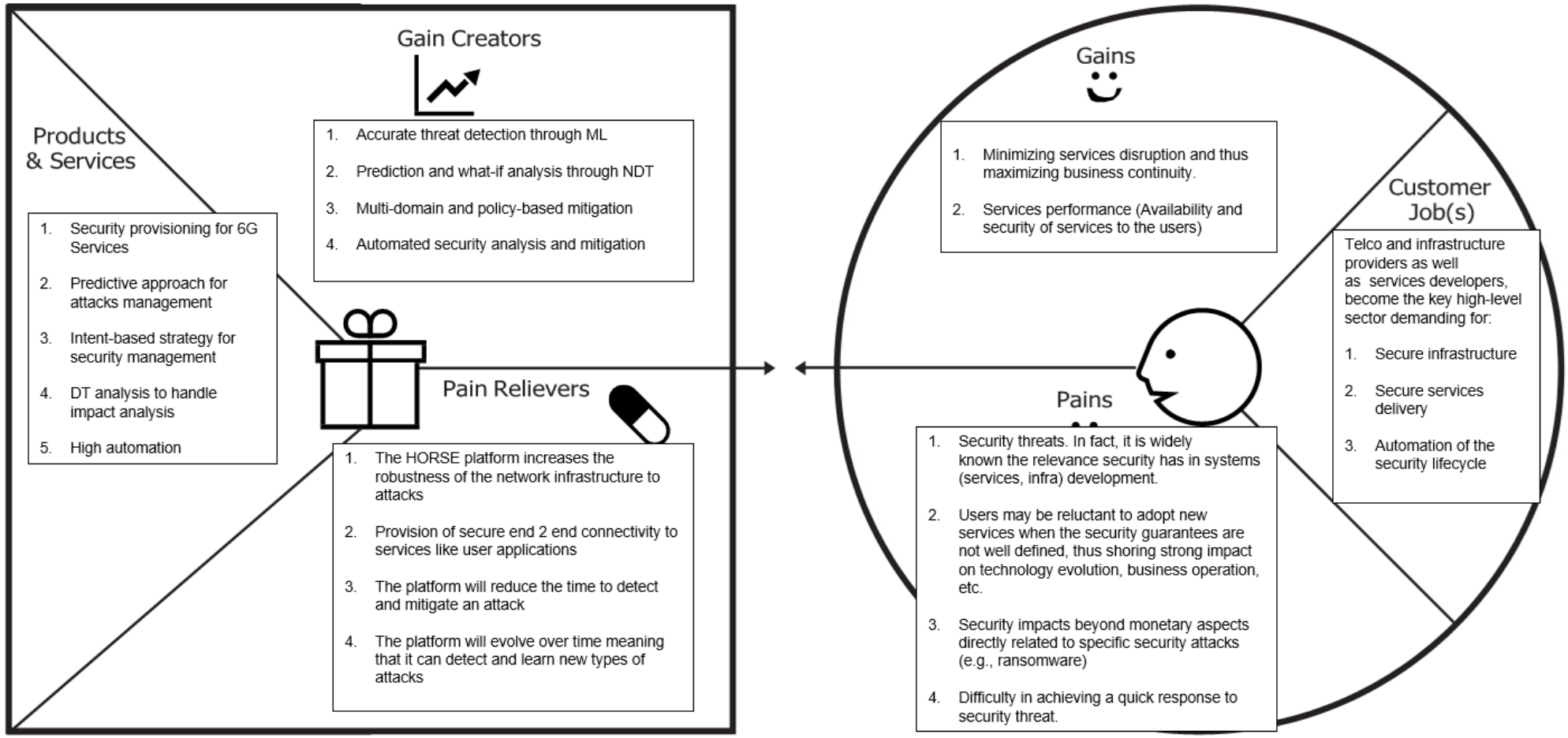
KER1 – HORSE Platform

MARKET DEFINITION CANVAS



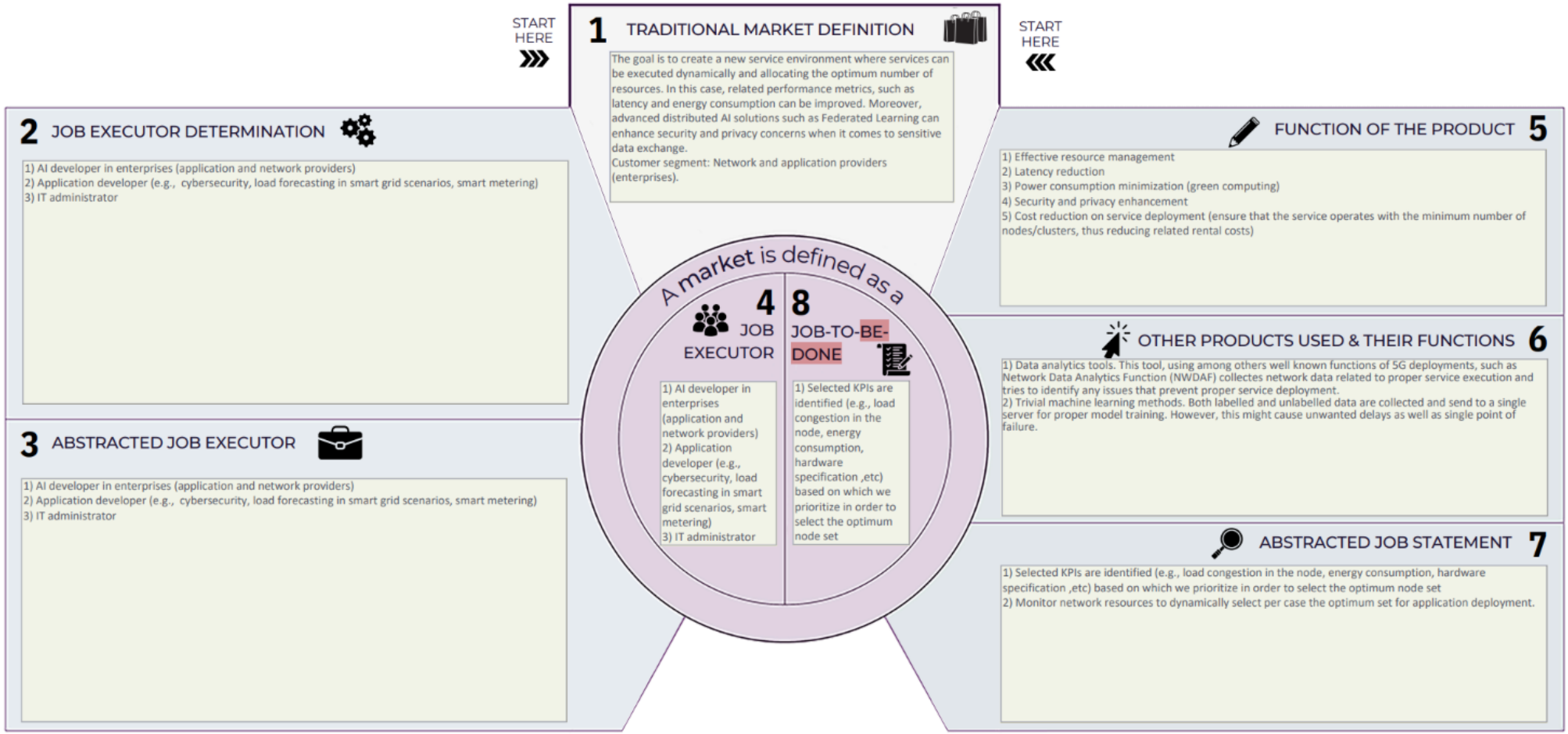
The Value Proposition Canvas

Customer Segment: Network managers in telecommunication enterprises



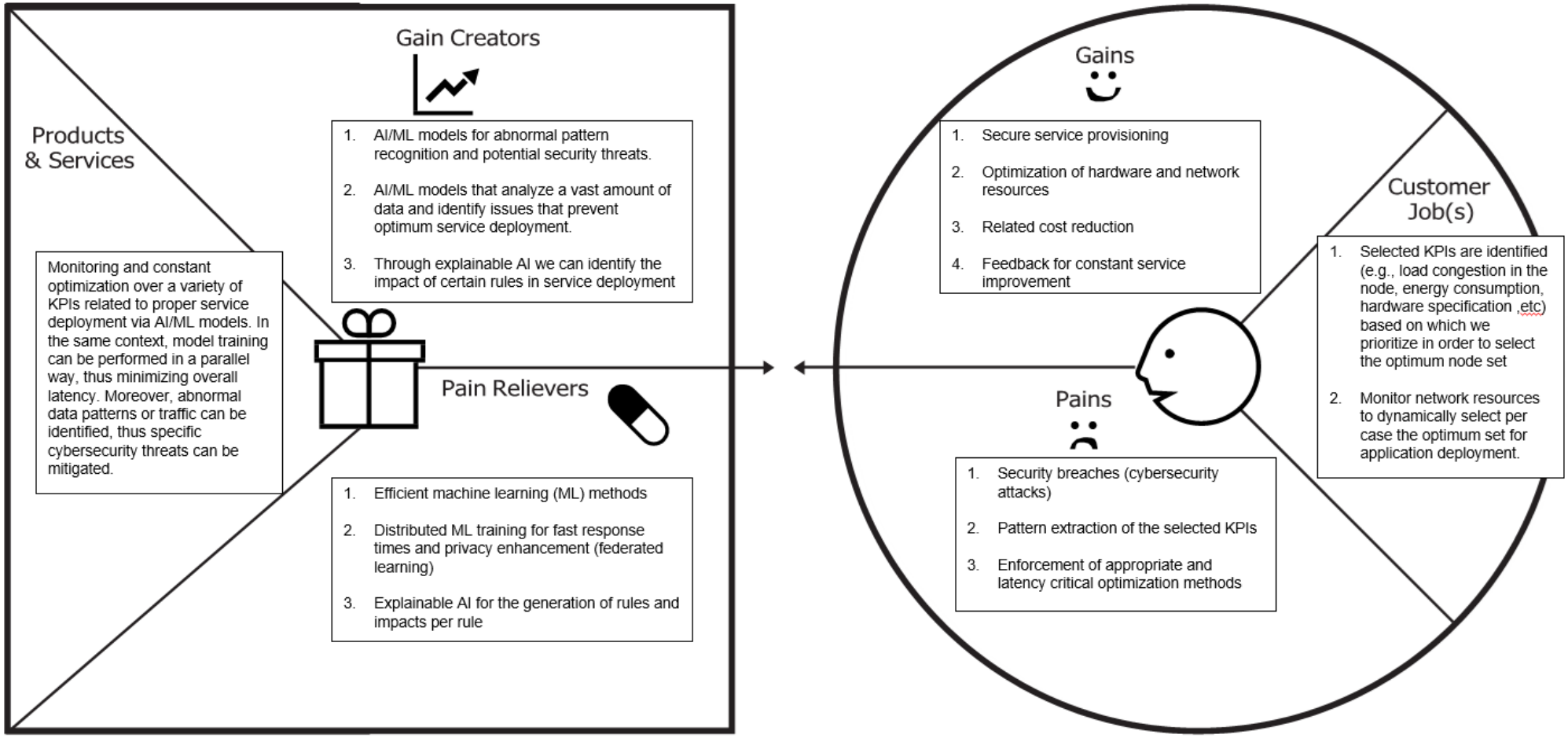
KER2 – Distributed AI Engine for Services Preassesment

MARKET DEFINITION CANVAS



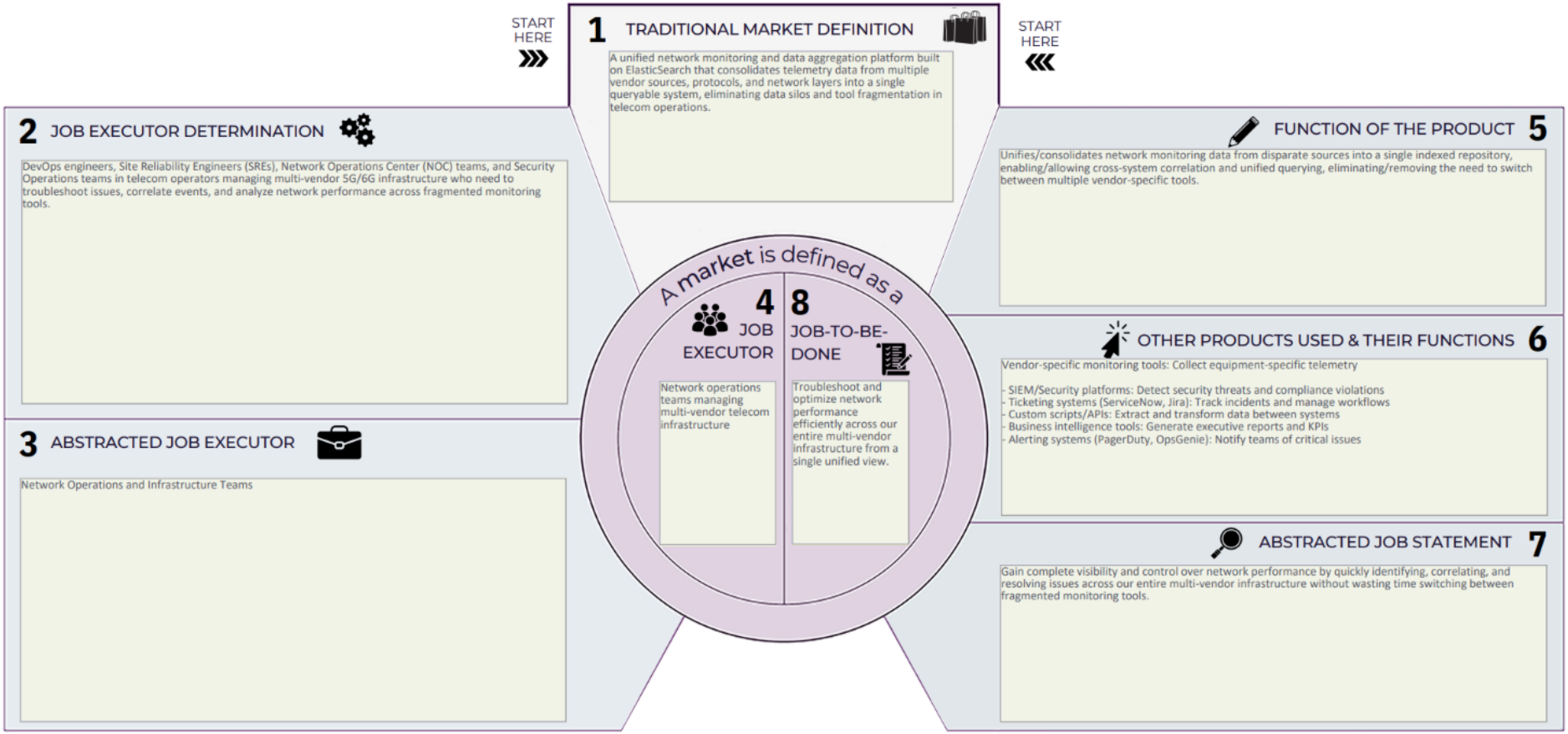
The Value Proposition Canvas

Customer Segment: AI developer in application and network enterprises



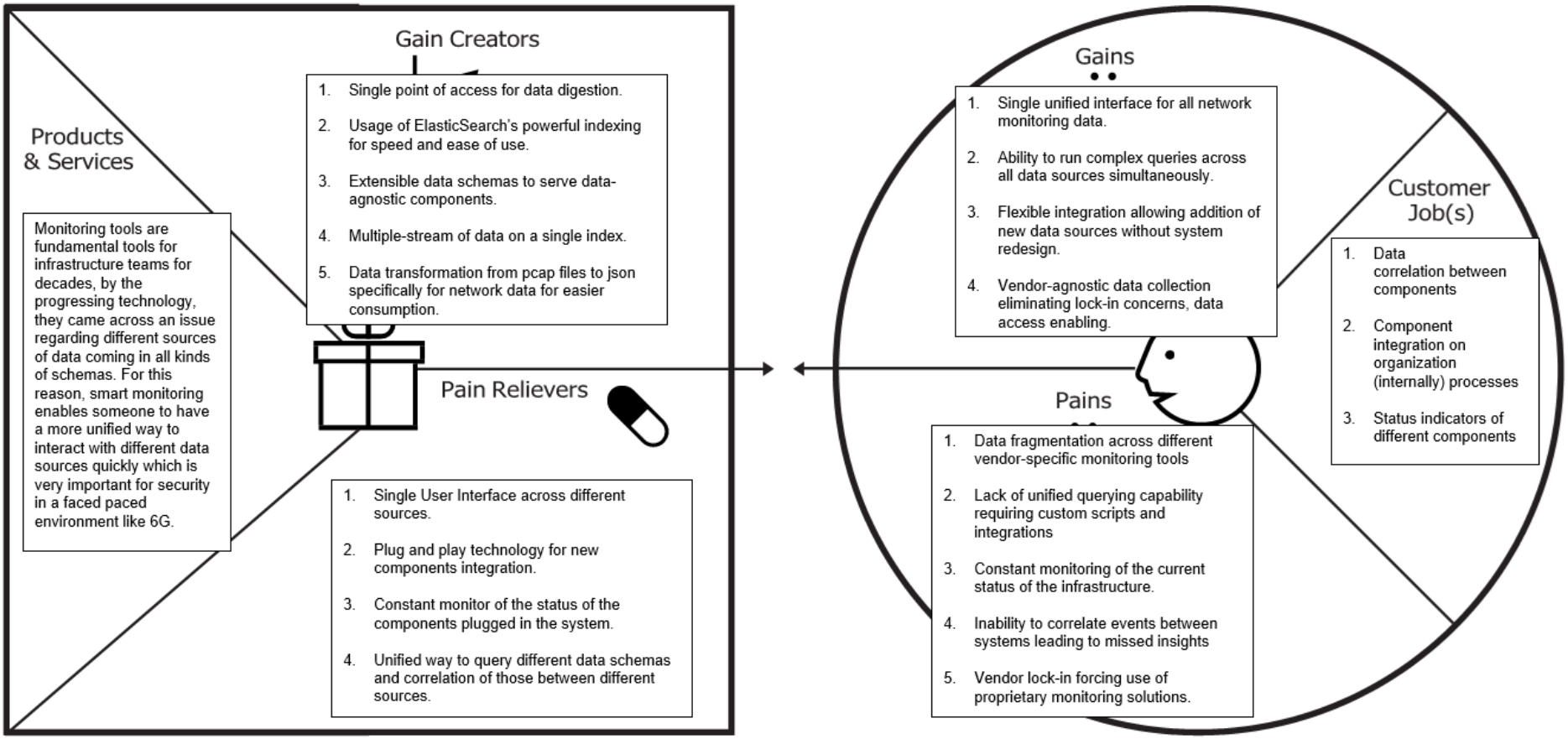
KER3 – Smart Monitoring (SM)

MARKET DEFINITION CANVAS



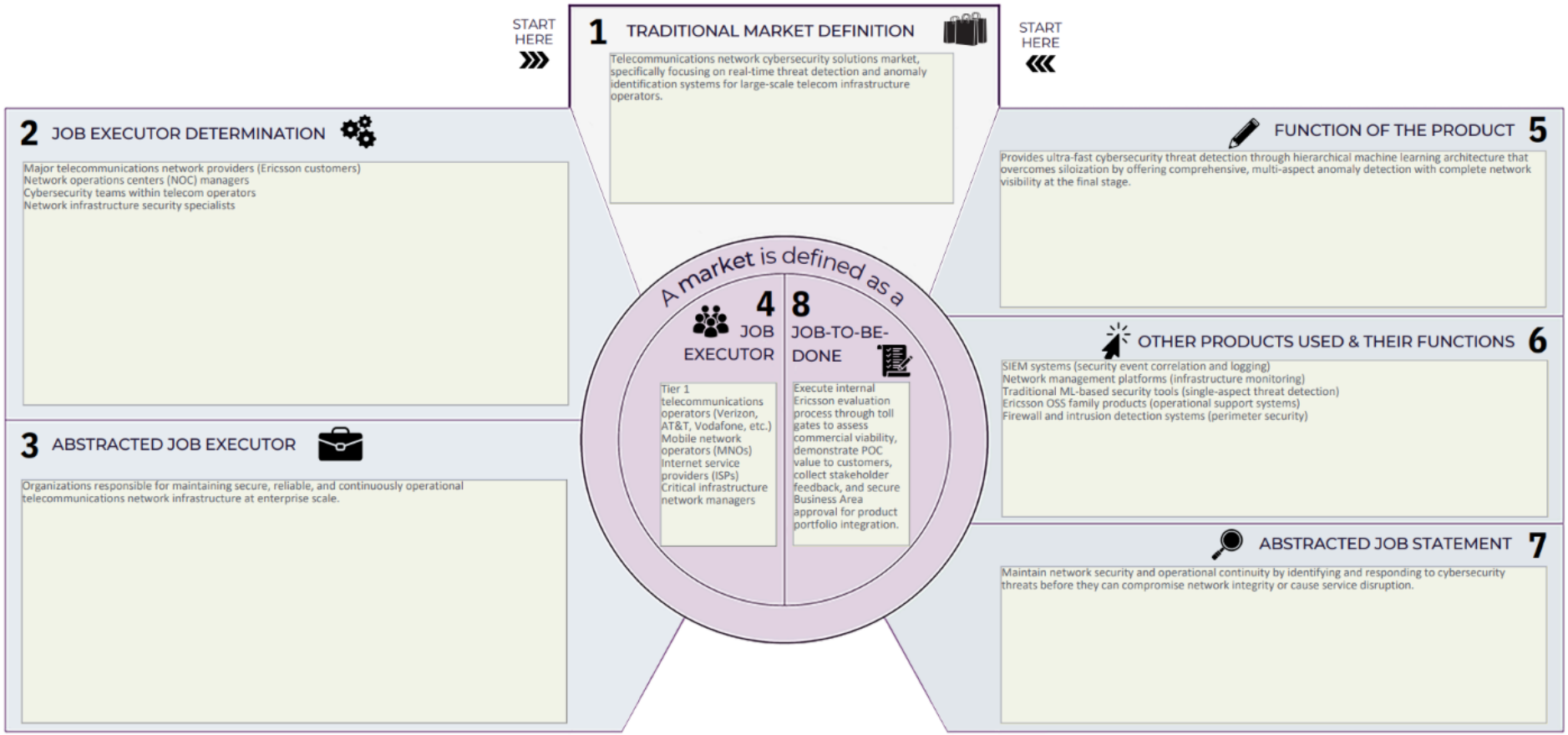
The Value Proposition Canvas

Customer Segment: DevOps teams in large telco organizations, struggling with fragmented monitoring tools and data silos



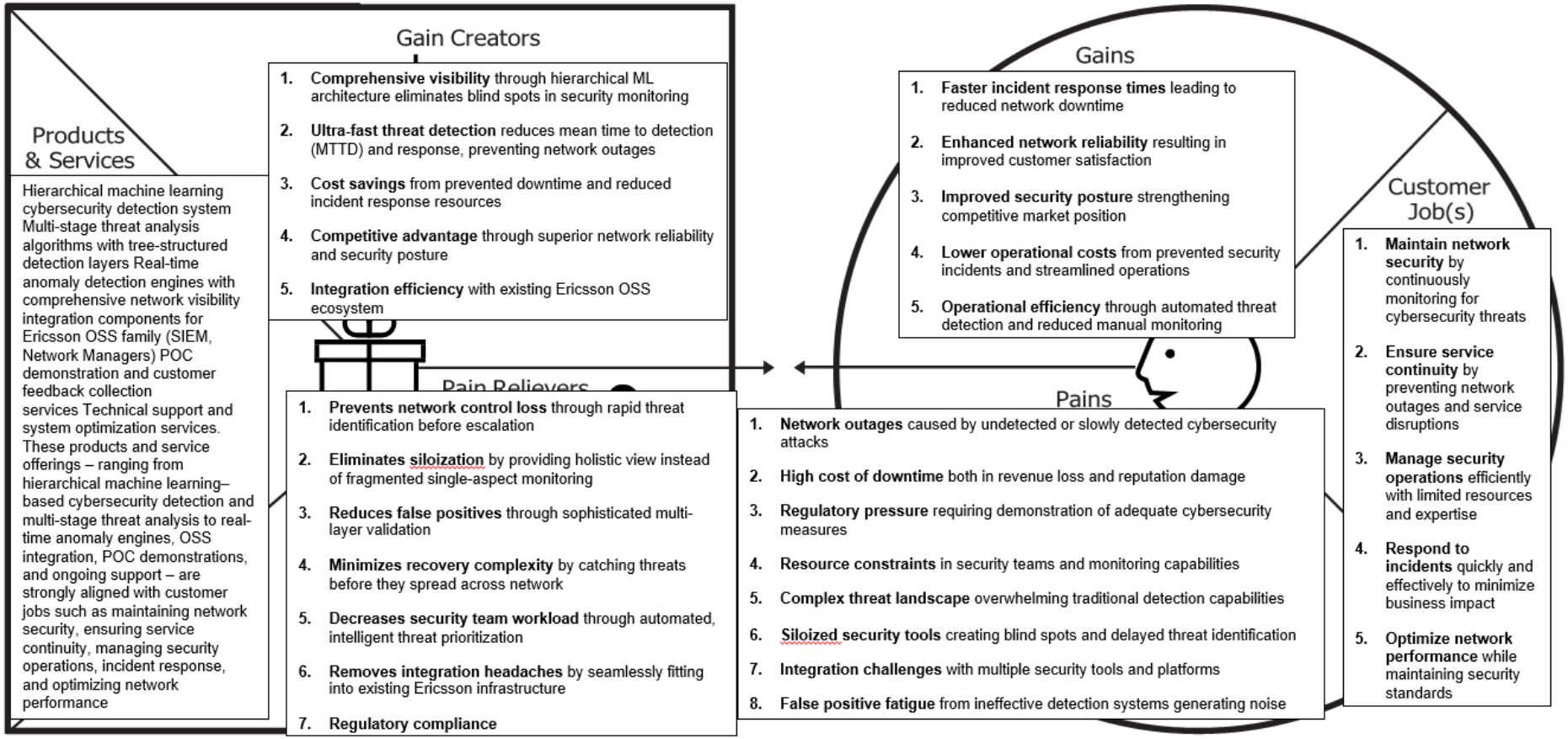
KER4 – Threat detector and mitigation engine

MARKET DEFINITION CANVAS



The Value Proposition Canvas

***Customer Segment: Network operations and cubersecurity teams in* Major telecommunications network providers**



KER5 – Intent-Based Secure cross-Domain Orchestrator

MARKET DEFINITION CANVAS

START HERE

1 TRADITIONAL MARKET DEFINITION

What is the product/service/idea you seek to innovate?

The Intent-Based Secure cross-Domain Orchestrator includes a set of tools to logically and physically interact with the infrastructure elements to provide a secure crossdomain orchestration. The interaction will be handled through a proper mapping of high-level intents into security workflows able to react to security threats and vulnerabilities.

START HERE

2 JOB EXECUTOR DETERMINATION

Who's using the product to get a job done?

Telecommunication providers and security analysts: Can use the orchestrator to automate incident response, seamless mitigation action enforcement and vulnerability management.

Network and IT Administrators: Can leverage the orchestrator to translate high-level security intents into consistent policies, streamline infrastructure management, enforce compliance, and adapt to evolving business and security requirements.

Customer segments: Telecommunication, cloud and IT service enterprises

3 ABSTRACTED JOB EXECUTOR

What overarching term can be used to classify all the categories of people using the product to get a job done

Security operations stakeholders

A market is defined as a

4 JOB EXECUTOR

A group of people

Telecommunication providers, Security analysts, Network and IT Administrators

8 JOB-TO-BE-DONE

The job get they are trying to get done

Automate and orchestrate security operations across multiple domains to rapidly respond to and mitigate security threats.

FUNCTION OF THE PRODUCT 5

What job does the product/service/idea you want to innovate get done? Format all job statements as: verb/object of the verb/contextual clarifier

It automates security workflows across multiple domains

It orchestrates security policies in complex IT environments

It transforms high-level security mitigation/prevention actions into enforceable commands suitable for heterogeneous infrastructures

OTHER PRODUCTS USED & THEIR FUNCTIONS 6

What other products do people use in conjunction with the product? What job does each of the other products get done?

SIEM systems like IBM QRadar (https://www.ibm.com/products/qradar) which aggregate security alerts for centralised monitoring and analytics

Threat intelligence platforms like Anomali (https://www.anomali.com/) which collect threat intelligence data to inform detection and response workflows

ABSTRACTED JOB STATEMENT 7

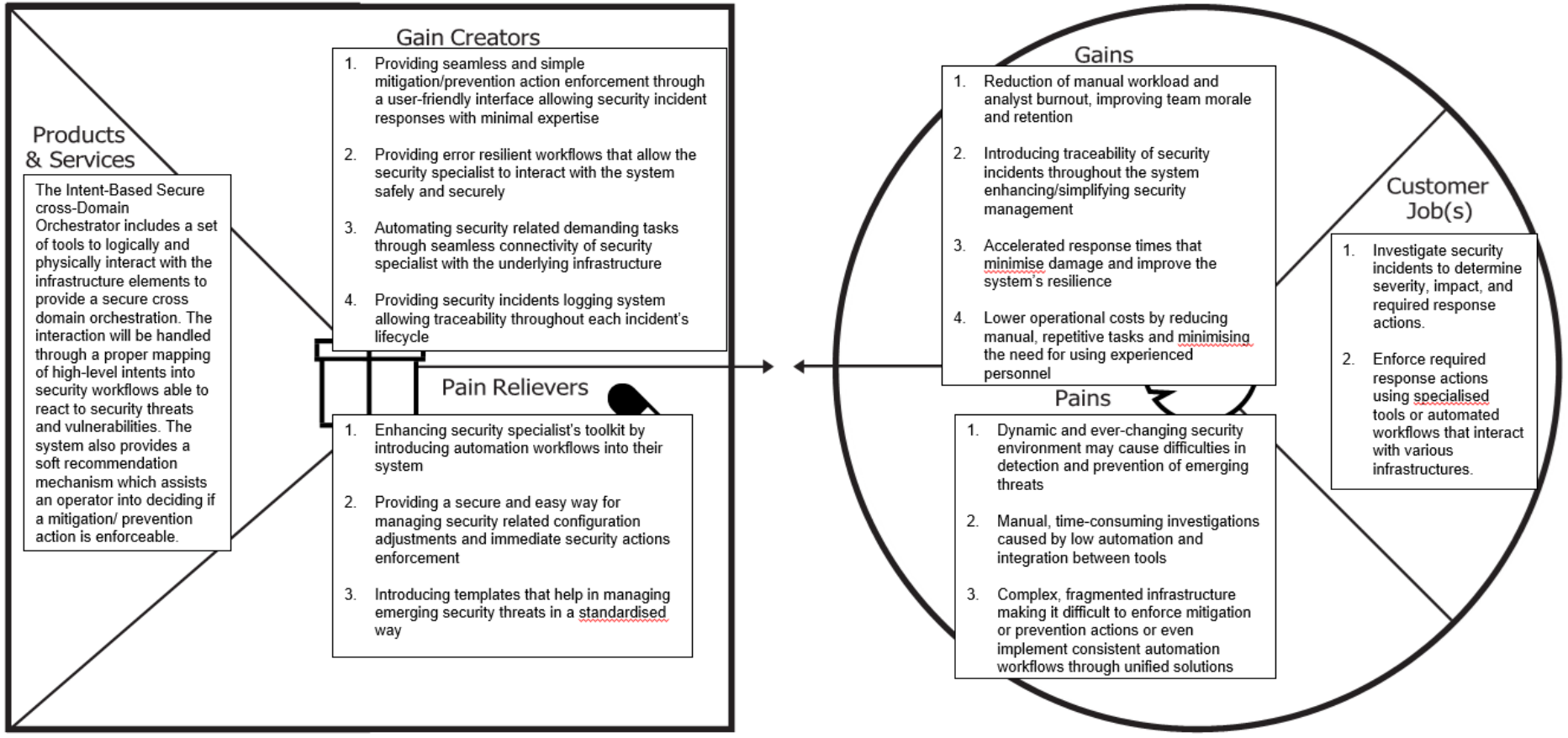
When looking at the market through the job executor's eyes, what core functional job do they say they are trying to get done?

Translate high-level security intents into automated, validated, and optimized cross-domain security workflows

Detect/respond to security threats rapidly and consistently across complex, distributed infrastructure

The Value Proposition Canvas

Customer Segment: Security operations teams within large telecommunications enterprises



KER 6 - End to end Proactive Secure Connectivity Manager (ePEM)

MARKET DEFINITION CANVAS

START HERE

1 TRADITIONAL MARKET DEFINITION

Creating a sophisticated, intelligent, and proactive orchestration service for future 6G networks. The innovation embodied by the ePEM is a novel Operations Support System (OSS) module and related service mechanisms aimed at AI-assisted end-to-end proactive secure connectivity management. The core innovation is the Availability of an end-to-end secure connectivity manager, which operates as an OSS module based on the Open Source MANO orchestrator.

START HERE

2 JOB EXECUTOR DETERMINATION

The actors and systems using the ePEM to perform its job can be categorized into the external commercial end-users who deploy and manage the network services, and the internal intelligent components of the HORSE platform that rely on the ePEM for execution.

Customer segments:
Network operators: Network managers
Cloud provides: Cloud service managers (checking the status of the network and infrastructure)
Tecommunication companies

3 ABSTRACTED JOB EXECUTOR

1. Network Operators and Service Providers: This covers entities responsible for building, maintaining, and selling connectivity or applications based on the infrastructure: Mobile Network Operators (MNOs), Over-the-Top (OTT) providers, and telecommunication companies/service providers.
2. Technology Providers and Developers: These groups integrate and enhance the core platform components: ICT vendors/providers, cybersecurity providers/function providers, and system integrators and software vendors.
3. Industrial and Vertical Users: These rely on the secure, orchestrated services managed by the ePEM: users from vertical sectors, and industrial sectors, such as those involved in the Light Rail Transit (SS-LRT) and Extended Reality (R22XRI) use cases, which rely on the reliable and secure connectivity provided by HORSE.

A market is defined as a

4 JOB EXECUTOR

Operators, technology providers, and high-level decision-makers responsible for managing and securing complex, multi-domain 6G networks.

8 JOB-TO-BE-DONE

The job get they are trying to get done. Ensuring secure, reliable, and proactively managed service deployment across heterogeneous 6G infrastructure, minimizing disruption and maximizing business continuity.

5 FUNCTION OF THE PRODUCT

- Manage/service orchestration/for multi-tenancy and resource deployment.
- Provide/secure framework/that can span across multiple domains and applications.
- Coordinate/work/of infrastructure domain building blocks.
- Dynamically enforced security mechanisms/according to QoS/QoE requirements and network load.
- Process/requests/for network slice lifecycle management.
- Support/recursive deployment/of functional components for high heterogeneity
- Support/resource self-configuration/for end-to-end connectivity.

6 OTHER PRODUCTS USED & THEIR FUNCTIONS

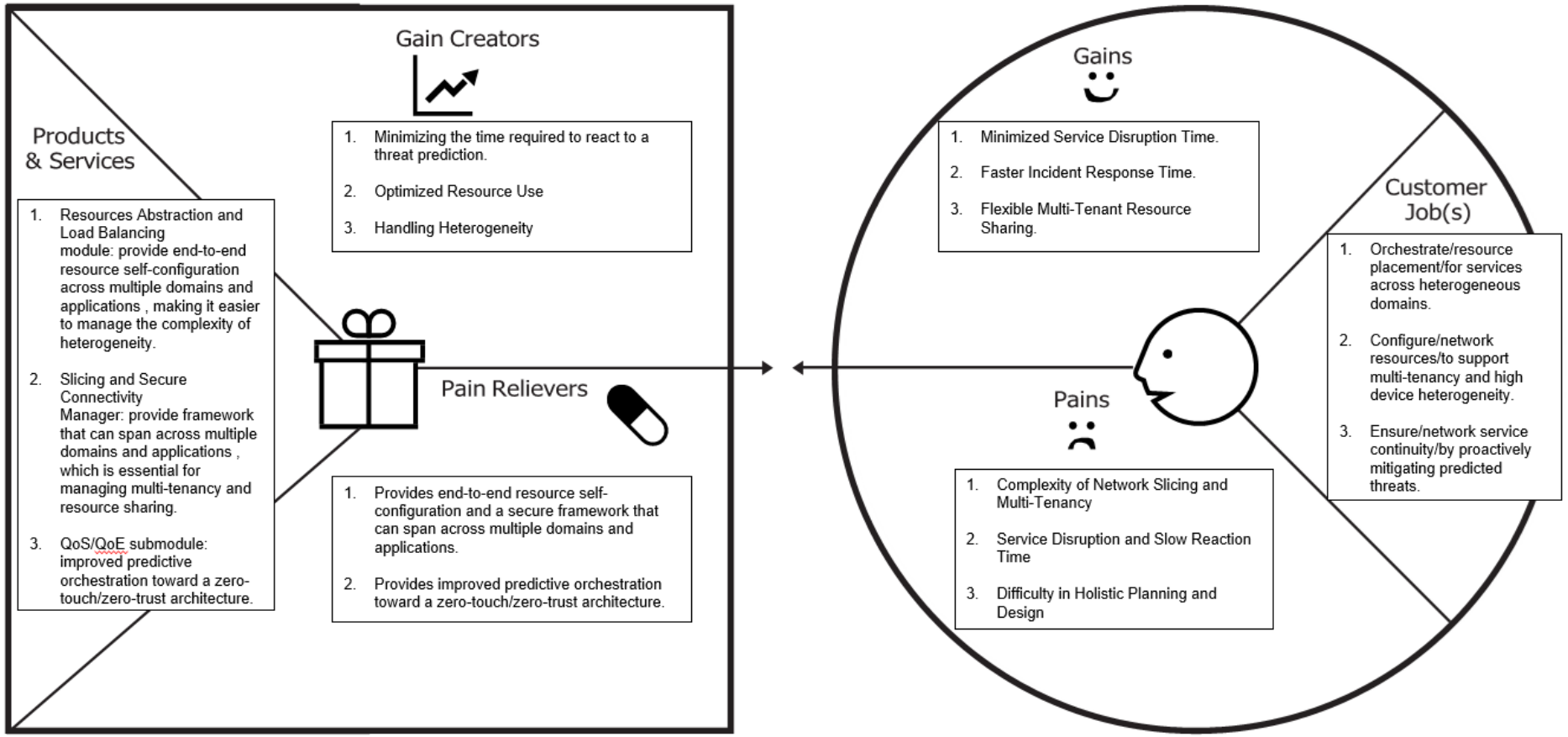
- Reliability, Trust and Resilience Provisioning (RTR) (NorthBound Interface): maps intents and policies decided by the intent-based components into specific actions that the ePEM must execute for secure resource orchestration.
- Domain Orchestrators Connectors (DOC) (SouthBound Interface): exploited by the ePEM as its SouthBound Interface to physically implement configurations, instantiate resources, and control slices across various infrastructure segments.

7 ABSTRACTED JOB STATEMENT

- Manage/all functions and operations/required for service placement over heterogeneous infrastructure.
- Provide/secure framework/that can span across multiple domains and applications.
- Assure/end-to-end connectivity/with predefined security levels per service slice.
- Dynamically update/enforced security mechanisms/according to QoS/QoE requirements and network load.

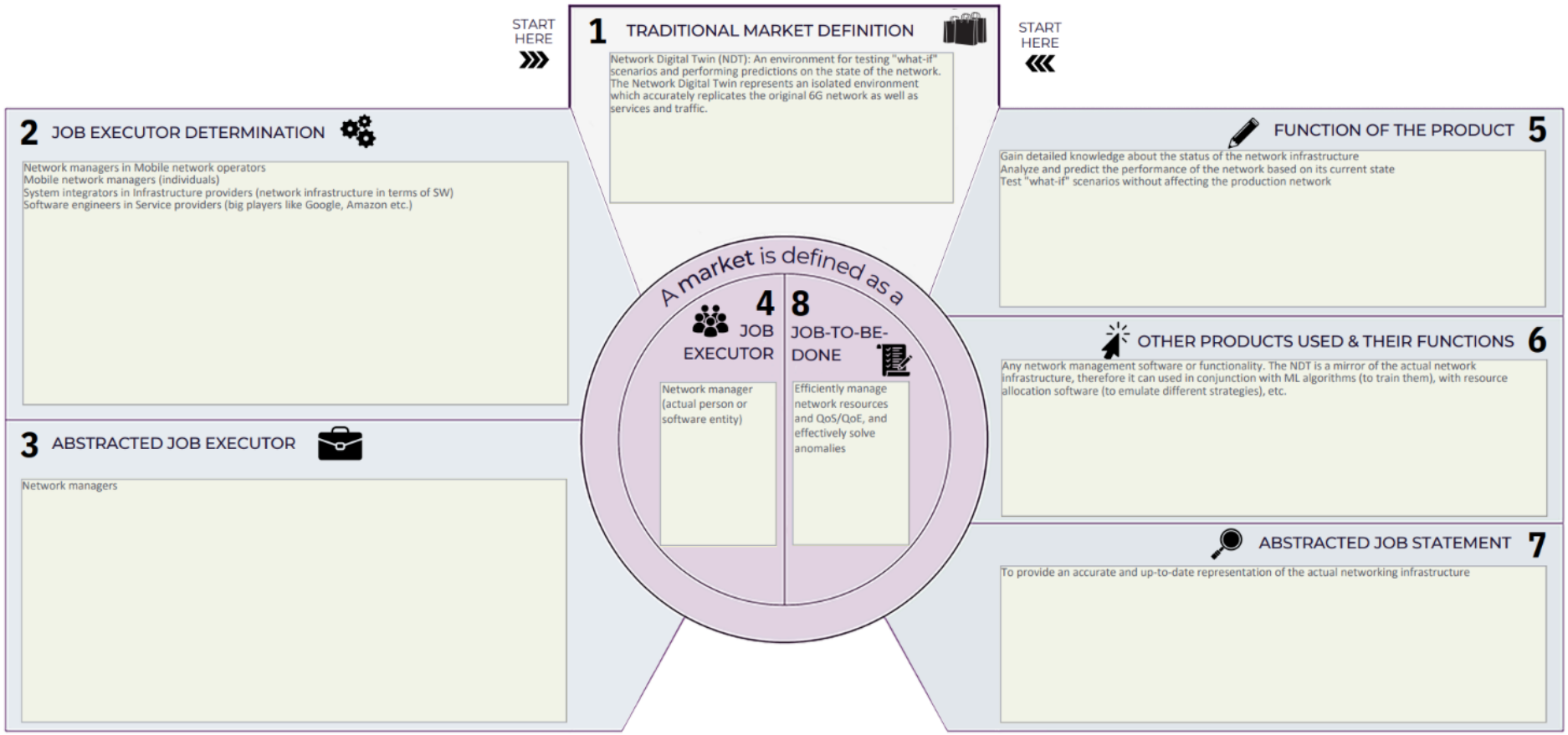
The Value Proposition Canvas

Customer Segment: Network managers in Mobile Network Operators (MNOs)



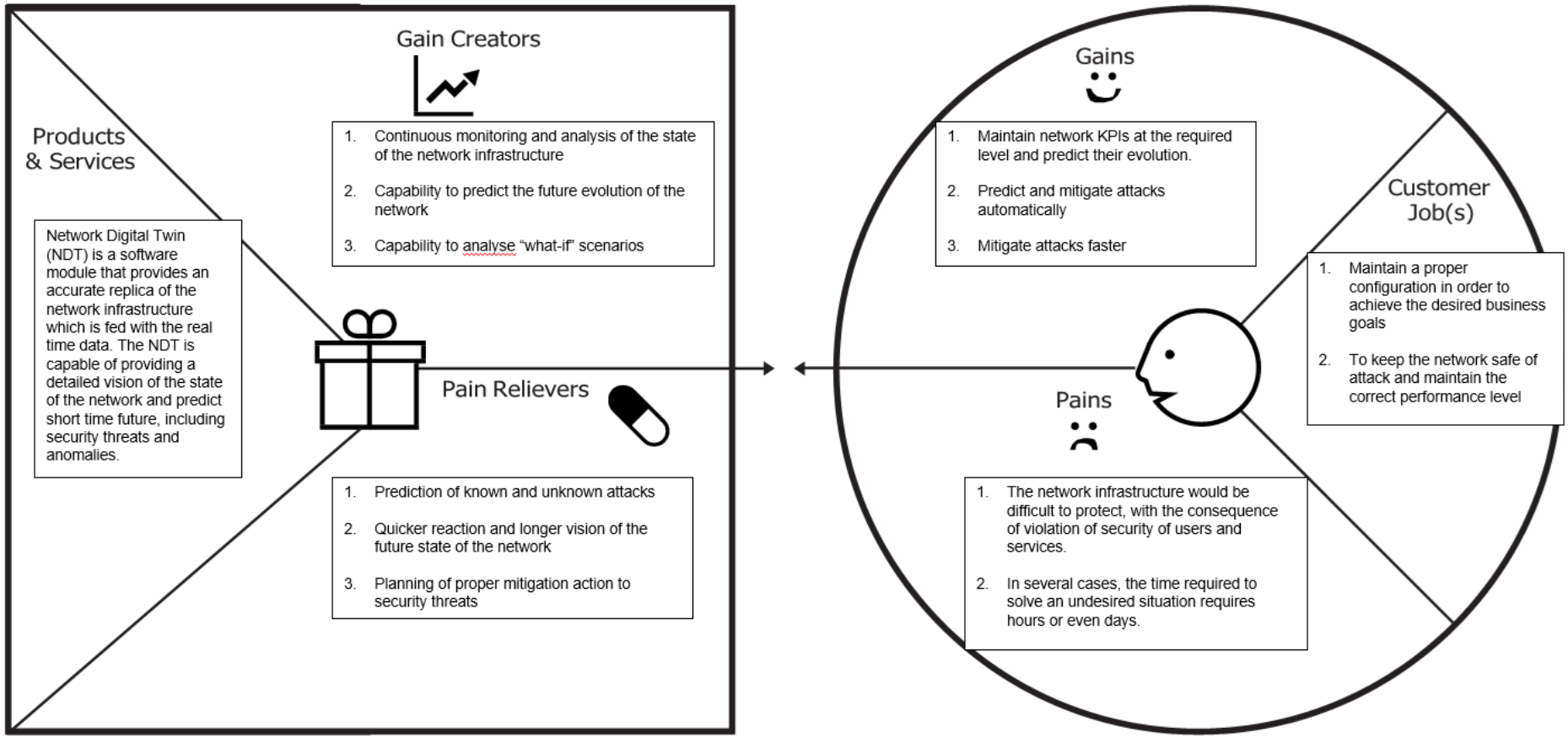
KER 7 – Network Digital Twin

MARKET DEFINITION CANVAS



The Value Proposition Canvas

Customer Segment: Network managers in Mobile network operators



13 Appendix D – Module C templates

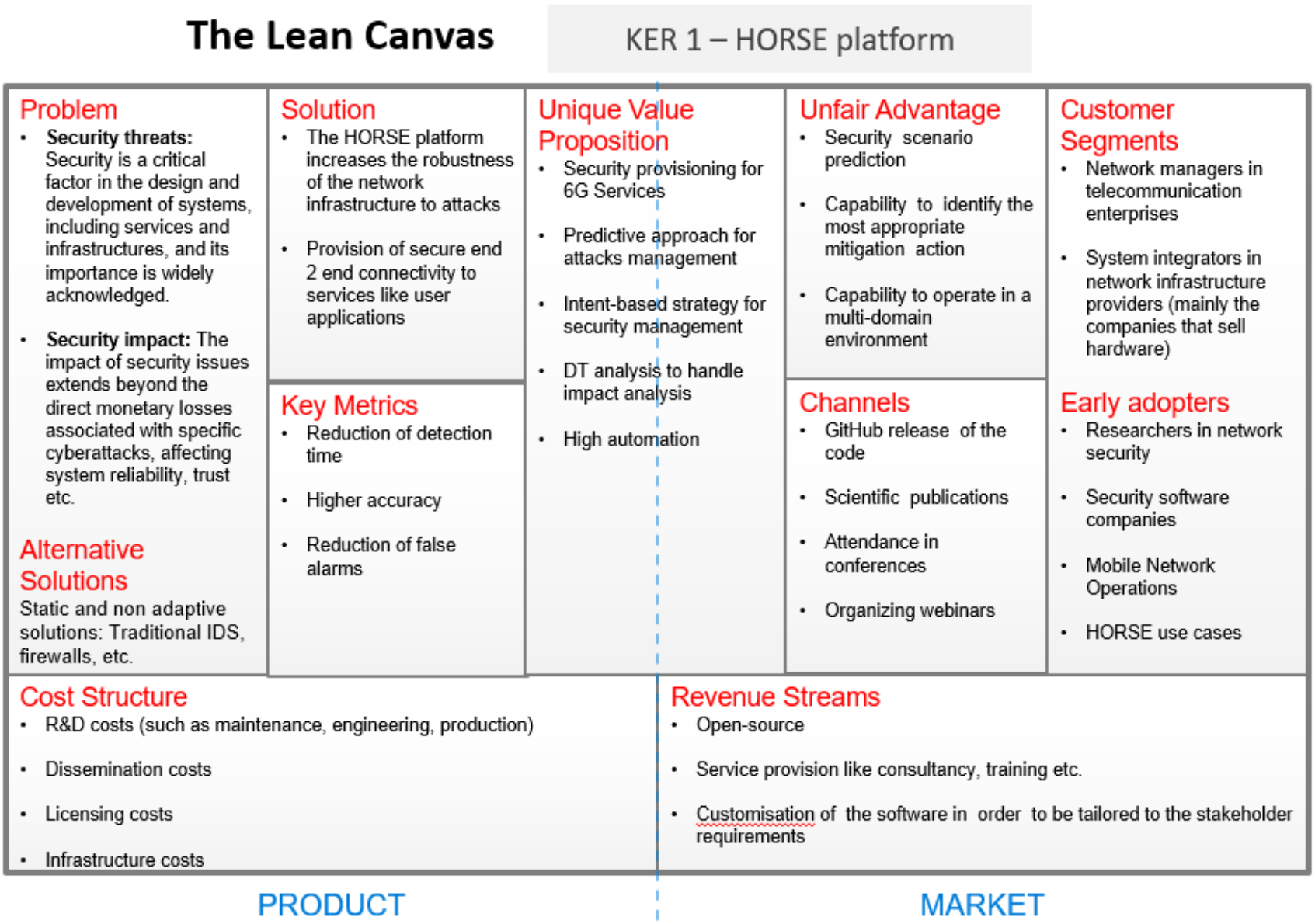
KER 1 – HORSE Platform

Exploitation roadmap for KER 1 – HORSE Platform	

Actions	• Search for funding opportunities (will start 1 month after the end of the project)
	• Engineering of the HORSE platform architecture (will start 1 month after the end of the project)
	  ○ Interfacing with physical infrastructure
	  ○ Securing internal interfaces among the modules
	  ○ Coordinating the further R&D activities of each Module
	• Discussions for a joint business plan with the other consortium partners (will start 6 months after the end of the project)
	• Identification of potential business partners in order to start collecting requirements (will start 6 months after the end of the project)
	• Dissemination activities in order to continue the community building for the platform (IEEE, ICC, NFVSDN conference etc.) (will start 6 months after the end of the project)
	• Customer development and validation activities (will start 8 months after the end of the project)

Roles	• Responsible for the KER exploitation and coordinating the further R&D activities: CNIT • Partners: ALL other HORSE partners will support the above activities

Milestones	• Funding opportunity(ies) detected • New functionalities applied • Joint exploitation / business strategy agreed among the consortium partners • Business partner(s) identified • A publication will be presented in a conference
Costs	During the first year after project CNIT will have the following costs: • R&D costs (such as maintenance, engineering, production): 15.000 – 25.000€ • Dissemination costs: around: 2000€ per conference • Licensing costs (either from the other consortium partners or third parties): 5.000 - 10.000€ • Infrastructure costs: 3.000 - 5.000€
Revenues	The HORSE platform will be launched as open-source and we will think about providing services like consultancy, training etc and also maintenance in our potential customers but the focus will be in R&D activities in order to be more technically mature. So, it's hard to provide a number of revenues at this stage.
Other sources of coverage	Requested financial resources to cover costs: partners` own budget, other project grants, national/regional incentives.



Risk Assessment Map for KER1 - HORSE platform

	Description of Risks	Degree of criticality of the risk related to the final achievement of this Key Exploitable Result. Please rate from 1 to 10 (1 low- 10 high)	Probability of risk happening Please rate from 1 to 10 (1 low - 10 high)	Risk Grade	Potential intervention	Estimated Feasibility/Success of Intervention Please rate from 1 to 10 (1 low- 10 high)	Conclusion
	Partnership Risk Factors						
1	Disagreement on ownership rules among the consortium	*2*	*3*	**6**	Substituting the partner	*6*	**Control.**
2	Key partners may leave	*7*	*3*	**21**	Try to find another big player to support the platform	*8*	**Control.**
	Technological Risk Factors						
3	Worthless result: better technology/ methodology exists	*7*	*2*	**14**	Perform additional R&D on the platform	*7*	**Control.**
4	Fail to neutralise new forms of attacks (e.g. zero-day attacks)	*6*	*3*	**18**	Continuous updates in the software	*8*	**Control.**
	Market Risk Factors						
5	Nobody buys the product. Typically, part of a bigger system (network management, network security)	*5*	*5*	**25**	Need to build alliance with software developers specialized in security in 5G/6G	*5*	**Between Control & No Action**
6	Not meeting the expectations of the customer segment	*6*	*4*	**24**	Frequent validation and feedback from stakeholders/ customers	*8*	**Control.**

	IPR/Legal Risk Factors						
7	The consortium cannot reach an agreement on IPR	*7*	*3*	**21**	Discussions with partners and form of a consortium based IPR strategy	*7*	**Control.**
	Financial/Management Risk Factors						
8	Limited financial and human resources from the consortium for further development, dissemination, maintenance and other activities	*5*	*4*	**20**	Preparation of a funding plan from each partner	*7*	**Control.**
	Environmental/Regulation/Safety risks						
9	Product does not comply with the standards	*5*	*2*	**10**	Need for further design phases	*8*	**Control.**

KER2 – Distributed AI Engine for Services Preassesment

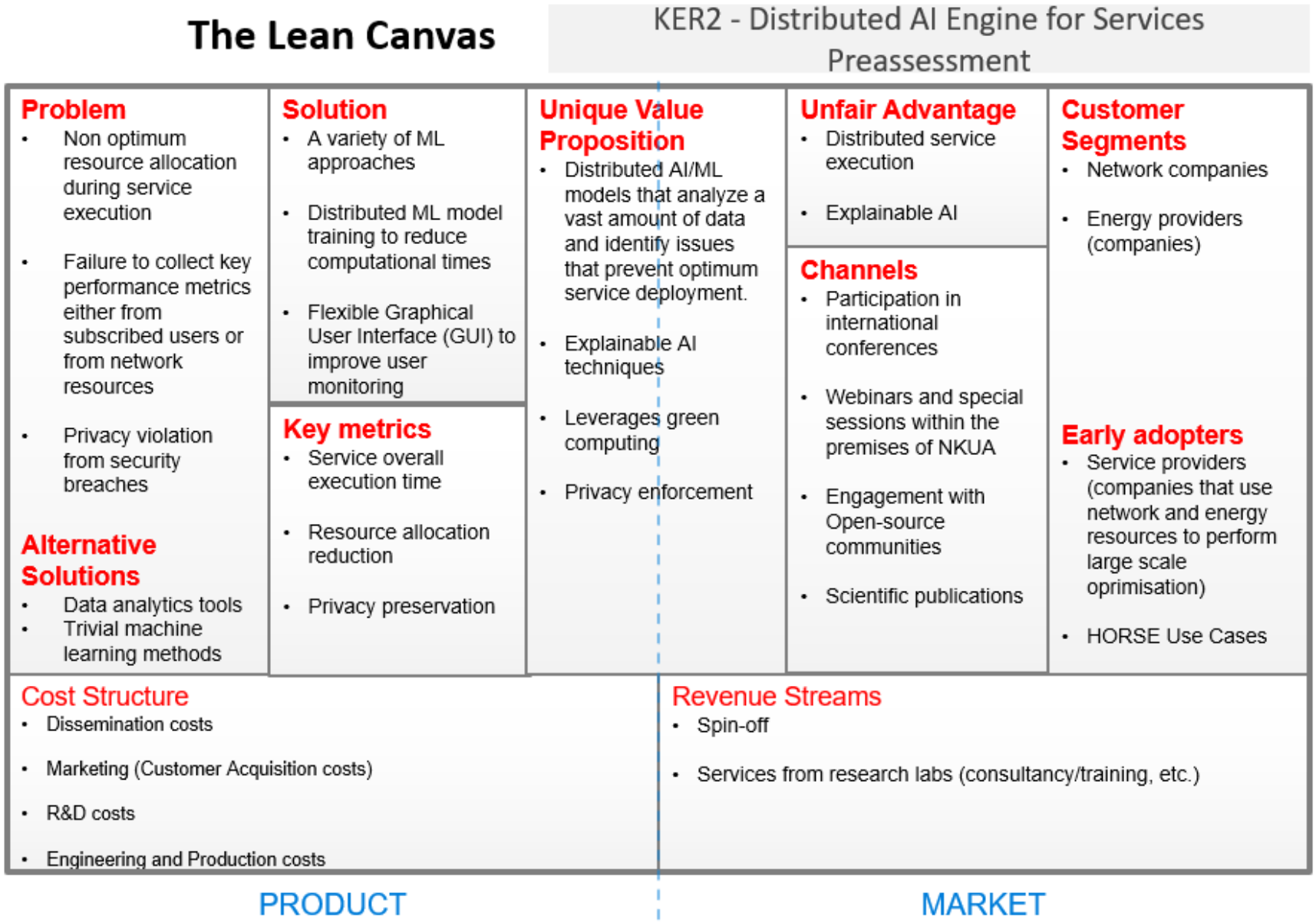
Exploitation roadmap for KER2 – Distributed AI Engine for Services Preassesment	

Actions	• NKUA will search for new funding opportunities (will start 1 month after the end of the project)
	• NKUA is planning to host webinars and special sessions regarding the functionality of the KER and how specific advantages can be achieved (will start 3 months after the end of the project).
	• NKUA will contact network and energy providers either from the Greek or the European market to clearly identify their needs and how these can be addressed via the KER (will start 4 months after the end of the project).
	• Start the formal copyright registration for KER2 (will start 6 months after the end of the project)
	• Further research and development in order to meet the requirements of stakeholders and increase TRL (will start 6 months after the end of the project). Those activities may include:
	  ○ Integration of more advanced ML approaches according to the analysis of stakeholder's requirements
	  ○ Enforcement of more robust security mechanisms

Roles	• The role of the NKUA will be to identify specific needs from related companies as well as to organize and promote dissemination activities. • NKUA is also planning to collaborate with companies that promote AI solution within the business market.

	• NKUA will be the responsible organization for the KER's exploitation roadmap
Milestones	• Identification of possible funding opportunities • Identification of all interested stakeholders • Organization/participation in dissemination events • Set of requirements (functional and non-functional) from the above stakeholders to identify the working environment of the distributed AI engine • Tangible performance metrics improvement from the service providers that will make use of the KER, • Formal copyright registration • Further R&D to reach TRL6-7.
Costs	• Marketing and dissemination costs (e.g. Participation in at least three (3) international conferences to promote the KER (estimated cost approximately 2000 euros per conference) • R&D: 1000-2000€/month • Infrastructure and maintenance: 6000-10000€
Revenues	• Service of the KER will be provided on an open-source basis. • NKUA is expecting in a time period from 1 up to 3 years from the end of the project to establish a spin-off.

	• Revenues from offering paid services via research labs All revenues will be calculated at a later stage
Other sources of coverage	The NKUA team is actively participating in various EU funded projects where its main role is the development of AI/ML approaches for services and resources optimization. To mention a few, these include the ICOS project (https://www.icos-project.eu/, resource optimization in the IoT-Edge-Cloud continuum, the OASSES project (https://oasees-project.eu/, decentralized AI/ML solutions) as well as the TARDIS project (https://project-tardis.eu/, trustworthy and Resilient decentralised intelligence for edge systems. The aim is to continue the participation in other EU-funded projects.



Risk Assessment Map for KER2 - Distributed AI Engine for Services Preassessment

	Description of Risks	Degree of criticality of the risk related to the final achievement of this Key Exploitable Result. Please rate from 1 to 10 (1 low- 10 high)	Probability of risk happening Please rate from 1 to 10 (1 low - 10 high)	Risk Grade	Potential intervention	Estimated Feasibility/Success of Intervention Please rate from 1 to 10 (1 low- 10 high)	Conclusion
	Partnership Risk Factors						
1	Difficulty in collecting enterprise data due to certain privacy policies	*5*	*5*	**25**	Face to face meeting with the involved personnel to explain the data collection process and stress the fact that preserves anonymity	*8*	**Control.**
2	Delays in the revision process of high-quality journal articles	*7*	*8*	**56**	Additional dissemination publications in international conferences as well, where response times can be predicted with a higher accuracy	*8*	**Action!**
	Technological Risk Factors						
3	Zero-day attacks	*7*	*7*	**49**	Release of a new product version, software update	*10*	**Control.**
4	Short technology lifecycle due to rapid technology of cybersecurity landscape	*8*	*6*	**48**	Continuous ML model refinement, adaptation to multiple areas (e.g. Network security, telcos)	*9*	**Control.**
	Market Risk Factors						

5	Not meeting the expectations of the customer segments	*8*	*5*	**40**	Frequent validation with customers, feedback from customers	*9*	**Control.**
6	Competitive landscape (Explainable AI)	*8*	*7*	**56**	Model refinement and improvement of user monitoring	*8*	**Action!**
	IPR/Legal Risk Factors						
7	Issues with formal declaration of IP protection	*5*	*6*	**30**	Early study of the procedures of IP protection	*8*	**Control.**
	Financial/Management Risk Factors						
8	Limited financial and human resources for development, dissemination, maintenance etc.	*8*	*6*	**48**	Preparation of a funding plan, participation of Post graduation students via their theses, participation in EU-funded projects, university research labs	*9*	**Control.**
	Environmental/Regulation/Safety risks						
9	Non/limited compliance with network security standards	*8*	*5*	**40**	Continuous monitoring and alignment with network security standards	*8*	**Control.**

KER 3 – Smart Monitoring (SM)

Exploitation roadmap for KER 3 – Smart Monitoring (SM)	
Actions	• Search for new funding opportunities (will start 1 month after the end of the project) • Adjust the Smart Monitoring into our own tools for better knowledge and testing (will start 1 month after the end of the project) • Research on other possible data types that SM can digest and transform to JSON (will start 2 months after the end of the project) • Research different markets for exploitation of the solution outside of the 6G scope (will start 4 months after the end of the project) • Participation in Dissemination events (will start 5 months after the end of the project) • Finalisation of a business and exploitation plan (will start 6 months after the end of the project) • Initiate the process of formal IP mechanism registration (will start 7 months after the end of the project)
Roles	• SPHYNX will be responsible for the exploitation and further R&D activities of KER3
Milestones	• Identification of possible funding opportunities • Fully integrated to SPA platform as a monitoring tool (At least 3 different data sources included, and 2 different data types)

	• Develop and provide different data ingestion mechanism for different data types (At least 1 more data type (other than PCAP) for native data ingestion within SM) • Further identification and communication of key stakeholders in more market areas (min 1 organisation in the next 12 months) • Conduct a legal advisor to initiate the formal IP registration (during the next 12 months)
Costs	• R&D costs: 40,000 - 80,000€ • Marketing costs (in terms of customer engagement): 3,000 – 4,000€ • Dissemination costs (along with other STS tools): 4,000 – 5,000€
Revenues	During the commercialisation of SM, the foreseen revenues in the first year may be (rough estimation): • Services (consultancy/training, etc.): 10,000 – 30,000€ • Maintenance: 5,000 – 10,000€
Other sources of coverage	• EU follow-up funding (inclusion of the technology in new EU-funded projects) • Own resources

The Lean Canvas

KER3 - Smart Monitoring

Problem
- Integrating a new telemetry source (e.g., new VNF, new sensor, new log type) currently requires significant development effort and system downtime.
- Downstream modules (AI, Orchestration) are too dependent on the specific format of collected data, making changes complex and brittle.
- Vendor lock-in forcing use of proprietary monitoring solutions.

Alternative Solutions
- Custom-made solutions for each individual vendor / data point. (Speculation for 6G environments)

Solution
- Ingestion Framework
- Schema-Agnostic Elastic Indexing
- Simple Data Registration API
- Module-based extensibility

Key Metrics
- Time-to-Integrate (TTI) a New Data Source
- Data Ingestion Throughput
- Coverage Extensibility (In terms of new possible trends in 6G)

Unique Value Proposition
- Modularity through plug and play architecture. For different data sources, utilizing Elastic Search's indexing
- Fast indexing on the saved data through which also supports Elastic Search's indexing API.
- Single source of truth for data through the for every component attached to the Smart Monitoring
- Data transformation for Packet Capture data to indexable format (JSON) which will help on analysis and enable querying on the data

Unfair Advantage
- Easily to adapt to new infrastructure.
- Combining different data types into one specific (JSON currently) for easier ingestion from the other components or usage from users

Channels
- Attend workshops / conferences
- Write scientific papers and journals
- Industrial events, and present it to stakeholders

Customer Segments
- System and DevOps Engineers in telco enterprises
- Network security enterprises

Early adopters
- DevOps on Telecommunication operators
- HORSE Use Cases

Cost Structure
- Dissemination costs
- Marketing (Customer Acquisition costs)
- R&D costs
- Engineering and Production costs

Revenue Streams
- Services (consultancy/training, etc.)
- Maintenance

PRODUCT | MARKET

Risk Assessment Map for KER3 – Smart Monitoring

	Description of Risks	Degree of criticality of the risk related to the final achievement of this Key Exploitable Result. Please rate from 1 to 10 (1 low- 10 high)	Probability of risk happening Please rate from 1 to 10 (1 low - 10 high)	Risk Grade	Potential intervention	Estimated Feasibility/Success of Intervention Please rate from 1 to 10 (1 low- 10 high)	Conclusion
	Partnership Risk Factors						
1	Loss of Key personnel or expertise: Staff turnover or limited technical continuity could lead to loss of know-how and further development delays.	*8*	*5*	**40**	Knowledge transfer, documentation, cross-training among team members	*9*	**Control.**
	Technological Risk Factors						
2	Unknown 6G network data throughput: Uncertainty in future 6G networks regarding the actual data throughput and latency which may cause underperformance of SM	*6*	*7*	**42**	Check scalability of the system based on demands, testing using synthetic 6G traffic, optimise Elasticsearch indexing to adapt dynamically to throughput variations	*5*	**Between Control & No Action**
3	Better technologies: Rapid evolution of observability and analytics technologies in the 6G network.	*9*	*8*	**72**	Stay up to date with new technologies in 6G and update as needed, monitor emerging observability frameworks, modular architecture	*8*	**Action!**
	Market Risk Factors						

4	Performance lower than market needs: SM might not meet the 6G expectation in terms of speed, affecting market acceptance	*4*	*8*	**32**	Constant talk with the stakeholders to know their needs at any point, definition of specific KPIs, refinement of data ingestion tools	*4*	**No Action'**
5	Insufficient market visibility and promotion: Limited communication efforts	*7*	*5*	**35**	Participate in scientific conferences, publish scientific papers, promotion via digital channels	*7*	**Control.**
	IPR/Legal Risk Factors						
6	Unclear exploitation or licensing strategy may cause delays in commercialisation	*6*	*5*	**30**	Define and validate a clear IPR protection and licensing strategy, consult legal advisors	*8*	**Control.**
	Financial/Management Risk Factors						
7	Post-project sustainability: SM may lack updates and long term-support in case of an incomplete business plan	*5*	*5*	**25**	Develop a complete sustainability plan, allocate resources for continuous updates	*8*	**Control.**
	Environmental/Regulation/Safety risks						
8	Changes in data protection laws (e.g. GDPR): New data protection frameworks might require architectural changes in SM	*9*	*7*	**63**	Monitor upcoming EU regulations, constant development based on those regulations	*9*	**Action!**

KER4 – Threat Detector and Mitigation Engine

Exploitation roadmap for KER4 – Threat Detector and Mitigation Engine	
Actions	Activities in the months following the end of the project will focus on engaging with Ericsson's Business Units (BU) and Customer Units (CU) to evaluate the integration of the new circuit into next-generation OSS products. This includes: • Preparing presentations and demonstrations in order to engage/attract stakeholders and/or existing customers (will start 2 months after the end of the project). • Start a number of internal processes (e.g. pre-acceptance of Ericson managers, collecting the requirements of the stakeholders, cost estimation etc.) in order to prioritise and implement the features of the next generation technologies of Ericsson (will start 6 months after the end of the project). • A number of steps for implementation, continuous integration, testing and validation of the technology (will start 8 months after the end of the project) • Testing the product in customers' premises (will start 18 months after the end of the project).
Roles	• The BU and CU of Ericsson hold decision-making authority for prioritization and potential integration of the circuit. • The laboratory that developed the circuit within the project acts in a consultative role, supporting demonstrations, technical explanations, and refinement of the solution.

Milestones	• Participation in dissemination events (like the Innovation Day and Technical Day organized by Ericsson) • Technical roadmap for development tailored to stakeholders' needs drafted and approved • New features developed in line with the roadmap • Pilot testing organized and implemented in customer premises
Costs	The costs for the actions mentioned above a cost estimation can be: • R&D costs in terms of features enrichment and integration of threat detector in existing Ericsson technologies: around 60PMs • Dissemination events: 5 – 6 PMs
Revenues	Revenues cannot be attributed to the circuit individually. OSS product revenues will be assessed in their entirety, reflecting the strategic role of OSS as part of Ericsson's complete network offerings. Revenue impact from this circuit is indirect, as its contribution helps strengthen OSS products and thus overall network sales, rather than generating standalone income.
Other sources of coverage	Current activities focus on evaluation and alignment rather than TRL increase or standalone commercialization. Resources are internal to Ericsson, leveraging BU and CU engagement, laboratory consultation and existing budgets for technical refinement, demonstration, and customer interactions. Also, a source of coverage may be future EU projects in order to be more technologically mature.

The Lean Canvas

KER4 – Threat Detector and Mitigation Engine

Problem
- Need to detect cyber security threats as quickly as possible
- Ability to detect new or zero-day attacks
- Existing solutions are siloed, creating integration and harmonization issues
- Slow response and higher operational cost due to multiple parallel detectors

Alternative Solutions
- Multiple independent detectors operating in parallel
- Siloed outputs requiring harmonization
- Slower detection and less adaptability to new attacks
- Higher deployment and maintenance costs

Solution
- Hierarchical multi-stage Machine Learning architecture
- Maximum visibility at egress stage
- Adaptive learning for detection of new/zero-day attacks
- Reduced false positives and faster detection times
- Fully integrable in next-generation OSS platforms

Key Metrics
- Average threat detection time
- False-positive rate minimization

Unique Value Proposition
- Real-time, adaptive detection of emerging cyber threats
- Hierarchical ML approach ensures highest visibility at critical points
- Integrated solution reduces operational complexity and improves responsiveness
- Enhances overall security posture of OSS platforms

Unfair Advantage
- Proprietary hierarchical ML architecture developed
- Deep integration capability with OSS products
- Existing access to customer feedback and live operational data through CU and BU engagement
- Expertise and support from project laboratory as technical consultant

Channels
- Ericsson OSS sales channels and account management
- Customer engagement via Business Units (BU) and Customer Units (CU)
- Dedicated demonstrations and workshops for strategic customers
- Integration into full OSS product lifecycle (e.g., ENM upgrades)

Customer Segments
- Telecom operators using Ericsson OSS solutions
- Large-scale network operators
- Early adopters within strategic customer accounts prioritized by BU/CU
- Customers seeking high TRL OSS solutions with integrated innovative features

Early adopters
- Strategic operators already engaged with Ericsson BU/CU
- Customers participating in pilot programs and OSS trials
- Network operators interested in enhanced security and real-time threat detection
- Key accounts where new OSS product upgrades are planned

Cost Structure
- Costs considered at OSS product level, not per circuit
- Distribution & deployment handled via OSS lifecycle processes
- Engineering and R&D for ENM and next-gen OSS upgrades
- Staff and laboratory consultation for integration and demos
- Compliance, permits, and internal approvals managed by BU/CU

Revenue Streams
- OSS product sales (primary revenue)
- Services including consultancy, training, and integration
- Ongoing maintenance contracts for OSS products
- Indirect revenue from strengthened OSS product competitiveness in full network solutions

PRODUCT | MARKET

Risk Assessment Map for KER4 – Threat Detector and Mitigation Engine

	Description of Risks	Degree of criticality of the risk related to the final achievement of this Key Exploitable Result. Please rate from 1 to 10 (1 low- 10 high)	Probability of risk happening Please rate from 1 to 10 (1 low - 10 high)	Risk Grade	Potential intervention	Estimated Feasibility/Success of Intervention Please rate from 1 to 10 (1 low- 10 high)	Conclusion
	Partnership Risk Factors						
1	Ericsson will implement the circuit internally with no external partners	*1*	*1*	**1**	N/A: No Partnership will be in place	*1*	**No Action'**
	Technological Risk Factors						
2	The circuit may encounter technical issues during validation and integration with other OSS features, requiring fixes or adjustments	*7*	*6*	**42**	Conduct extensive validation tests for the circuit before integration Perform integration testing with other OSS features Iterative bug fixing and technical refinements	*8*	**Control.**
	Market Risk Factors						
3	Market conditions may affect adoption of OSS products, including strong competition, multi-vendor networks, open-source alternatives, and fluctuations in customer/government investment	8	7	**56**	Continuous monitoring of market trends and competitor offerings Engage with customers to validate demand and feature prioritization	7	**Action!**

					Adjust OSS product roadmap to maintain competitive advantage		
	IPR/Legal Risk Factors						
4	Low risk due to Ericsson's internal IP and legal expertise, but potential issues could arise if protections are incomplete or agreements are not correctly applied	*2*	*2*	**4**	Utilize Ericsson's internal legal and IP teams to review protection Ensure patents, licensing, and internal agreements are in place	*10*	**Control.**
	Financial/Management Risk Factors						
5	Minimal risk, as Ericsson has well-established processes to ensure budget, resource, and management control	*2*	*2*	**4**	Follow Ericsson's established financial and project management processes Ensure budgets, resources, and approvals are in place for all planned activities	*10*	**Control.**
	Environmental/Regulation/Safety risks						
6	Regulatory or safety compliance issues are unlikely due to Ericsson's dedicated teams, but oversight or updates in regulations could pose minor risks	*2*	*2*	**4**	Leverage dedicated regulatory and compliance teams Monitor changes in applicable laws and regulations Ensure all required approvals and certifications are obtained	*10*	**Control.**

KER5 - Intent-based Secure cross-Domain Orchestrator

Exploitation roadmap for KER5 – Intent-based Secure cross-Domain Orchestrator	

Actions	• Search for new funding opportunities (will start 1 month after the end of the project).
	• Further research and development in order to be more technologically mature (will start 1 month after the end of the project). More specifically:
	  ◦ Quality assurance and quality testing in multiple end-to-end tests in order to further validate the KER into different environments
	  ◦ Optimisation of the deployment pipelines in order to have seamless deployment in new use cases.
	• Participation in dissemination events in order to continue the community building around the KER (will start 6 months after the end of the project).
	• Identification of more early adopters/stakeholders (will start 7 months after the end of the project).
	• Further R&D activities in order to meet the stakeholders' requirements (will start 9 months after the end of the project).
	• Formal IPR registration (will start 9 months after the end of the project).

Roles	8BELLS will have full ownership and responsibility for post-project exploitation, R&D activities and protection of KER5
Milestones	• Detection of new funding opportunities

	• Prototype fully tested and optimised • Dissemination and communication strategy approved and released • Technical roadmap for future development drafted and approved • IPR strategy defined and approved
Costs	• R&D costs: 35,000 – 50,000€ • Infrastructure and software maintenance: 25,000 – 30,000€ • Marketing and dissemination: 13,000 – 16,000€
Revenues	Revenues cannot be calculated at this stage because the focus will be further R&D. The orchestrator will be incorporated in other products (either 8BELLS's or not), so the revenues will be calculated accordingly. However, we expect revenues from: • Licensing fees (from subscriptions) • Integration and customisation services • Support and maintenance contracts
Other sources of coverage	• EU follow-up funding (inclusion of the technology in new EU-funded projects) • 8BELLS own resources

The Lean Canvas

KER5 - Intent-based Secure cross-Domain Orchestrator

Problem
- Complex and fragmented infrastructures make it difficult to enforce consistent security workflows.
- Response actions are often manual, time-consuming, and require highly skilled personnel
- Dynamic, ever-changing security environments hinder detection and prevention of emerging threats.

Alternative Solutions
- SIEM systems like IBM QRadar
- Threat intelligence platforms like Anomali

Solution
- Automated security workflows and policy enforcement across heterogeneous domains.
- AI-powered (NLP and LLM-integrated) knowledge base for dynamic threat-mitigation pairing.
- Modular orchestration design adaptable to diverse network segments.
- Built-in recommendation mechanism for mitigation/prevention actions.

Key Metrics
- Number of automated workflows deployed successfully.
- Reduction in incident response time.
- Operational cost savings and reduced manual interventions.

Unique Value Proposition
- Faster and more consistent threat response through: intelligent threat mitigation beyond traditional rule-based systems.
- Providing a modular DOC design that adapts to diverse network segments, surpassing rigid, segment-specific solutions.
- User-friendly and resilient platform that reduces manual workload, operational costs, and complexity across heterogeneous infrastructures.

Unfair Advantage
- Integration of advanced NLP and LLMs enabling adaptive, context-aware threat mitigation—unmatched by traditional rule-based systems.
- Modular cross-domain design allowing seamless orchestration across heterogeneous infrastructures.

Channels
- Direct sales
- Partnerships with telco enterprises
- Demonstrations at industry events and cybersecurity conferences.
- Online promotional materials and technical documentation.

Customer Segments
- Security operations teams within large telecommunications enterprises.
- Cloud service providers and operators
- Enterprise IT departments

Early adopters
- HORSE use cases
- Telecommunications & Network Operators

Cost Structure
- Personnel costs (cybersecurity engineers, AI developers, and technical support)
- Maintenance costs (server, infrastructure etc.)
- R&D costs
- Integration costs
- Marketing costs

Revenue Streams
- Revenue from direct sales (mainly from subscriptions)
- Services (consultancy/training, etc.)
- Maintenance

PRODUCT | MARKET

Risk Assessment Map for KER5 – Intent-based Secure cross-Domain Orchestrator

	Description of Risks	Degree of criticality of the risk related to the final achievement of this Key Exploitable Result. Please rate from 1 to 10 (1 low- 10 high)	Probability of risk happening Please rate from 1 to 10 (1 low - 10 high)	Risk Grade	Potential intervention	Estimated Feasibility/Success of Intervention Please rate from 1 to 10 (1 low- 10 high)	Conclusion
	Partnership Risk Factors						
1	Lack of industrial partner for large-scale deployment and/or commercialisation.	*7*	*5*	**35**	Identify potential telecom or cybersecurity integrators in order to form alliances.	*7*	**Control.**
2	Loss of Key personnel	*8*	*5*	**40**	Knowledge trnasfer, documentation, cross-training among team members	*8*	**Control.**
	Technological Risk Factors						
3	Dependency on third-party or emerging technologies (e.g., AI models, orchestration frameworks).	*8*	*4*	**32**	Maintain modular architecture, document open interfaces for interoperability, ensure backup options.	*7*	**Control.**
4	Short technology lifecycle due to rapid 6G evolution.	*7*	*4*	**28**	Design 6G-ready modular architecture adaptable to future standards.	*8*	**Control.**
	Market Risk Factors						
5	Limited market uptake if performance/usability not meeting	*8*	*5*	**40**	Perform validation with foreseen early adopters (telecom	*7*	**Control.**

	the expectations of customer segments.				operators, cloud providers etc.) and integrate feedback.		
6	Competition from bigger players (e.g., Cisco, IBM).	*8*	*6*	**48**	Highlight AI-based intent translation and modular design as differentiators in go-to-market plan.	*7*	**Control.**
	IPR/Legal Risk Factors						
7	Legal risks related to integration with third-party software or data sources.	*6*	*4*	**24**	Ensure licensing agreements and GDPR-compliant data handling.	*8*	**Control.**
8	Freedom to operate: someone does not allow to use their technology	*7*	*3*	**21**	Try to use open-source tools	*8*	**Control.**
	Financial/Management Risk Factors						
9	Limited financial or human resources to sustain post-project development and commercialisation.	*8*	*6*	**48**	Prepare detailed exploitation roadmap and funding plan.	*7*	**Control.**
10	Delays in business plan preparation or weak market validation.	7	6	42	Assign internal exploitation lead, start communication with foreseen adopters for validation.	7	**Control.**
	Environmental/Regulation/Safety risks						
11	Non-compliance with cybersecurity or telecom regulatory standards (e.g., ETSI, ISO/IEC 27001).	*8*	*4*	**32**	Align with regulatory standards during development	*7*	**Control.**
12	Ethical or social concerns related to automated decision-making.	*6*	*3*	**18**	Include audit transparency mechanisms.	*8*	**Control.**

KER 6 - End to end Proactive Secure Connectivity Manager (ePEM)

Exploitation roadmap for KER 6 - End to end Proactive Secure Connectivity Manager (ePEM)	

Actions	• Search for new funding opportunities (will start 1 month after the end of the project).
	• Disseminate the ePEM via conferences, scientific publications etc. (will start in 3 months after the project)
	• Further R&D in order to become more mature (will start in 3 months after the project):
	  • To develop a blueprint dependency matrix in order to simplify the resolution of possible security problems that can arise in some services provided by the ePEM.
	  • Integrate some AI mechanisms in order to automatically create the blueprint dependency matrix checking the different available blueprints.
	• Identification of external partners, their requirements and realisation of a prototype with blueprints for different scenarios, technologies and infrastructure (will start in 6 months after the project).
	• Finalisation of a business plan (will start in 9 months after the project)
	• Start of exploitation, definition and implementation of the blueprints based on the stakeholders' needs (will start in 10 months after the project).

Roles	CNIT will have full ownership and responsibility for post-project exploitation, R&D activities and protection of KER6

Milestones	• Detection of new funding opportunities • Definition of AI mechanisms for automated blueprint generation. • Collection of requirements for blueprint matrix • List of specific stakeholders and their requirements • Draft of a business plan completed. • Exploitation strategy and deployment of ePEM in selected use cases
Costs	• Engineering costs for R&D activities: 20.000 € – 50.000 € / year • Infrastructure maintenance costs: 20.000 € – 40.000 € / year • Dissemination costs: 1.500 € per publication, 3.000 €/conference • Training costs: 3-6PMs for training a newcomer, (15.000 € – 30.000 €) • Realisation of a prototype with different blueprints: 20.000 euros / blueprint.
Revenues	The ePEM will be launched as open-source and we will think about providing services like consultancy, training etc and also maintenance in our potential customers but the focus will be in R&D activities in order to be more technically mature. So, it's hard to provide a number of revenues.
Other sources of coverage	Partners` own budget, other project grants, national/regional funding initiatives.

The Lean Canvas

KER 6 - End to end Proactive Secure Connectivity Manager (ePEM)

Problem
- Service Disruption and Slow Reaction Time
- Difficulty in Holistic Planning and Design

Alternative Solutions
- High Speed Encryptors from THALES for securing data in transit (fronthaul/midhaul/backhaul) and solutions like Luna HSMs and CipherTrust Manager for key management, encryption, and subscriber privacy in the 5G core.
- Red Hat enterprise open-source platforms such as OpenShift and RHEL, serving as the cloud-native foundation for running virtualized and containerized 5G core network functions (VNFs/CNFs).

Solution
- The blueprint functionality simplifies the integration without problems derived from new functionalities.
- The possibility to enable-disable temporary some services and functionalities without a direct impact on the whole system.

Key Metrics
- Improve of how to design and integrate a new service and functionality in the system
- Faster incident response processes.
- Minimising business disruption time.

Unique Value Proposition
- It provides end-to-end resource self-configuration across multiple domains and applications , making it easier to manage the complexity of heterogeneity
- It provides a framework that can span across multiple domains and applications , which is essential for managing multi-tenancy and resource sharing

Unfair Advantage
- To work only on a specific service without impaction the whole system
- Integrate different type of infrastructure / technologies (e.g. different Kubernetes clusters, OpenStack instances)

Channels
- Scientific publications
- Participation in conferences
- GitHub release of the open-source code

Customer Segments
- Mobile Network Operators (MNOs) and
- Telecomm. companies requiring secure, resilient 6G service orchestration.
- ICT Vendors/Providers and developers utilizing flexible APIs. Vertical industries with performance-critical needs (e.g., LRT, XR).

Early adopters
- Researchers
- Security software companies
- Mobile Network Operations
- Virtual Mobile Network Operators
- HORSE use cases

Cost Structure
- R&D costs
- Engineering costs
- Infrastructure maintenance costs
- Dissemination costs
- Training costs

Revenue Streams
- Open source
- Services (consultancy/training, etc)
- Maintenance

PRODUCT | MARKET

Risk Assessment Map for KER 6 - End to end Proactive Secure Connectivity Manager (ePEM)

	Description of Risks	Degree of criticality of the risk related to the final achievement of this Key Exploitable Result. Please rate from 1 to 10 (1 low- 10 high)	Probability of risk happening Please rate from 1 to 10 (1 low - 10 high)	Risk Grade	Potential intervention	Estimated Feasibility/Success of Intervention Please rate from 1 to 10 (1 low- 10 high)	Conclusion
	Partnership Risk Factors						
1	Loss of Key personnel	*7*	*4*	**28**	Add a new member on the team with specific training on ePEM.	*8*	**Control.**
	Technological Risk Factors						
2	Worthless result: better technology/ methodology exists	*2*	*2*	**4**	Perform additional R&D on the customization and programmability of blueprints	*7*	**Control.**
	Market Risk Factors						
3	Nobody buys the product. Typically, part of a bigger system (network management, network security)	*3*	*5*	**15**	Need to build alliance with telecom and network operator with some specialization in security in 5G/6G	*5*	**Between Control & No Action**
	IPR/Legal Risk Factors						
4	Issues with formal declaration of IP protection	*4*	*3*	**12**	Early study of the procedures of IP protecton	*5*	**Between Control & No Action**

	Financial/Management Risk Factors						
5	Lack of endorsement from top management	*4*	*4*	**16**	Identify alternative partners	*5*	**Between Control & No Action**
	Environmental/Regulation/Safety risks						
6	Product does not comply with the standards	*5*	*2*	**10**	Need for further design phases (redisign the blueprint approach with to make compliant with the standards).	*8*	**Control.**

KER7 – Network Digital Twin (NDT)

Exploitation roadmap for KER7 – Network Digital Twin (NDT)	

Actions	• Search for new funding opportunities (will start 1 month after the end of the project).
	• Continuous dissemination through scientific papers and conferences (it will start in 1 month after the end of the project)
	• Further R&D activities to add new features (they will start in 3 months after the end of the project):
	  • Support for new security threats
	  • Automation deployment (e.g. automatic deployment/configuration of topology and attacks)
	• Identification of external partners and realisation of a prototype (it will start in 3 months after the end of the project)
	• Finalisation of the business plan (it will start in 6 months after the end of the project)
	• Start of exploitation, customization of the NDT engine to the stakeholders' needs (it will start in 9 months after the end of the project)

Roles	Responsible for the exploitation roadmap: CNIT and TID CNIT and TID will be able to exploit the KER separately, as in HORSE two NDTs are developed: one by CNIT and one by TID
Milestones	• Detection of new funding opportunities

	• Prepare presentations for international conferences • Update the release of the NDT (around M9 after the end of the project) • Prototype ready (around M12 after the end of the project) • Business plan drafted and approved (around M12 after the end of the project)
Costs	• Dissemination costs: for CNIT can be 5,000 -10,000€, for TID will be 5,000 – 10,000€ • R&D: for CNIT can be 15,000 – 30,000€, for TID can be 20,000 – 35,000€ • System maintenance costs: for CNIT can be 2,000 – 4,000€, for TID can be 2,000 – 4,000€
Revenues	The NDT will be launched as open-source and we will think about providing services like consultancy, training etc and also maintenance in our potential customers but the focus will be in R&D activities in order to be more technically mature. So, it's hard to provide a number of revenues.
Other sources of coverage	Partners` own budget, other project grants, national/regional funding initiatives.

The Lean Canvas

KER 7 – Network Digital Twin

Problem
- The network infrastructure would be difficult to protect, with the consequence of violation of security of users and services.
- In several cases, the time required to solve an undesired situation requires hours or even days.
- Better adapting the services to the network scenario

Alternative Solutions
- Network emulators and simulators (e.g. EVE-NG)
- Static and non adaptive solutions: Traditional IDS, firewalls, etc.

Solution
- Prediction of known and unknown attacks
- Quicker reaction and longer vision of the future state of the network
- Planning of proper mitigation action to security threats

Key Metrics
- Attacks detection accuracy
- Detection and mitigation time of attacks
- Network state prediction accuracy

Unique Value Proposition
The NDT helps network managers in mobile network operators who want to maintain a proper configuration in order to achieve business goals by reducing the difficulty of protecting the network infrastructure and help maintain network KPIs at the required level and predict their evolution.

Unfair Advantage
- Continuous interaction and synchronization with network infrastructure
- Accurate prediction and impact analysis of mitigation actions

Channels
- Scientific papers
- Participation in conferences
- Release of the code in GitHub
- Demonstrations and tutorials of the KER in conferences etc.

Customer Segments
- Network managers in Mobile network operators
- Mobile network managers (individuals)
- System integrators in Infrastructure providers (network infrastructure in terms of SW)
- Software engineers in Service providers (big players like Google, Amazon etc.)

Early adopters
- Researchers
- Security software companies
- Mobile Network Operations
- Virtual Mobile Network Operators
- HORSE Use cases

Cost Structure
- R&D costs
- Dissemination and communication costs
- Maintenance

Revenue Streams
- Open-source
- Services (consultancy/training, etc.)

PRODUCT | MARKET

Risk Assessment Map for KER7 – Network Digital Twin (NDT)

	Description of Risks	Degree of criticality of the risk related to the final achievement of this Key Exploitable Result. Please rate from 1 to 10 (1 low- 10 high)	Probability of risk happening Please rate from 1 to 10 (1 low - 10 high)	Risk Grade	Potential intervention	Estimated Feasibility/Success of Intervention Please rate from 1 to 10 (1 low- 10 high)	Conclusion
	Partnership Risk Factors						
1	A partner may leave.	*7*	*2*	**14**	Identification of a new partner to support the KER	*6*	**Control.**
	Technological Risk Factors						
2	Worthless result: better technology/ methodology exists	*2*	*2*	**4**	Perform additional R&D on the NDT	*7*	**Control.**
	Market Risk Factors						
3	Nobody buys the product. Typically, part of a bigger system (network management, network security)	*5*	*5*	**25**	Need to build alliance with software developers specialized in security in 5G/6G	*5*	**Between Control & No Action**
	IPR/Legal Risk Factors						
4	Issues with formal declaration of IP protection	*4*	*3*	**12**	Early study of the process	*5*	**Between Control & No Action**

	Financial/Management Risk Factors						
5	Lack of endorsement from top management	*4*	*4*	**16**	Identify alternative partners	*5*	**Between Control & No Action**
	Environmental/Regulation/Safety risks						
6	Product does not comply with the standards	*5*	*2*	**10**	Need for further design phases (redesign the blueprint approach with to make compliant with the standards).	*8*	**Control.**

14 Appendix E – Module D template

Business Plan for KER1 – HORSE platform

1. Executive summary

This Business Plan presents the exploitation and further development strategy of the HORSE Platform, a KER of the Horizon Europe HORSE project. The platform addresses the growing challenges of cybersecurity, automation, and resilience in next-generation 5G and 6G network environments, where highly distributed, software-defined, and heterogeneous infrastructures demand security solutions that go beyond traditional reactive approaches.

Briefly, the HORSE Platform introduces an AI-native, predictive, and intent-based security orchestration framework, integrating advanced machine-learning-driven threat detection, Network Digital Twin (NDT)–based pre-assessment of attacks and mitigation actions, declarative security policies, and automated cross-domain orchestration.

At the end of the HORSE project, **the platform reaches TRL 4–5**, having been demonstrated in operational pilot environments. Consequently, **this Business Plan does not target immediate commercialisation, but rather focuses mainly on continued research and technical consolidation**. In the short to medium term, the strategic objective is to progress toward TRL 6–7 through architectural hardening, expansion of mitigation-action databases, improvement of machine learning models, enhanced interoperability with physical and virtual infrastructures, and extensive validation in realistic environments. Moreover, CNIT as the coordinator of the project will take the responsibility to further coordinate all actions for the platform's maturity in the future.

From a market perspective, HORSE targets the rapidly expanding **cybersecurity and network security markets**, driven by the large-scale deployment of 5G infrastructures and the early transition toward 6G. Market trends highlight increasing demand for AI-driven threat detection, autonomous mitigation, digital twin–enabled resilience, and zero-trust architectures. While the sector is highly competitive and dominated by major global vendors, HORSE differentiates itself through its predictive security approach, intent-based orchestration, and pre-assessment of actions using NDTs—capabilities that remain limited or fragmented in existing solutions.

Beyond the target markets, the platform exhibits strong replicability and cross-sector applicability. Thanks to its modular and technology-agnostic architecture, HORSE can be adapted to any domain requiring secure, resilient, and intelligent networked infrastructures. Promising expansion areas include healthcare systems, smart grids and energy infrastructures, smart cities, industrial automation, transportation systems, and large-scale IoT ecosystems.

The Business Model of HORSE is currently research-driven and service-oriented. In the short term, exploitation focuses on open-source dissemination, community building, and service-based activities such as consultancy, system integration support, training, and customised deployments. Two long-term deployment modes are envisaged once sufficient maturity is achieved: (i) **HORSE-as-a-Service**, operated by intermediaries such as system integrators or service providers, and (ii) **on-premises deployments** for operators and enterprises requiring full control over security-sensitive infrastructures. Pricing strategies are expected to follow service-based or subscription-oriented models at later stages, once operational stability is ensured.

The operative plan foresees a structured, multi-year R&D roadmap combining consortium-wide integration activities with partner-specific maturation of individual components and supported by targeted dissemination, customer development and early adopter engagement, **without assuming immediate market entry**. Financial planning reflects the research-oriented nature of the platform, with estimated investments focused on R&D, infrastructure maintenance, dissemination, and coordination, while revenue projections are intentionally deferred until higher TRLs are achieved.

Continuity beyond the HORSE project is reinforced through follow-up initiatives such as the Horizon Europe MARE project, which builds directly on HORSE's architectural foundations and extends its proactive, intent-based, and pre-assessment security concepts. Also, some target calls mentioned in the end of this document which will further fund the evolution of the HORSE platform.

In the long term, the strategic ambition of the HORSE Platform is to evolve into a reference European open-source framework for predictive, automated, and AI-driven security orchestration for 5G/6G networks and beyond.

2. The organisation

Mission: To develop a modular, AI-native cybersecurity platform enabling predictive, automated and intent-based protection for 5G/6G networks, supporting operators, integrators and service developers in achieving end-to-end secure connectivity.

This business plan builds on KER1 - HORSE Platform, a key exploitable result of the Horizon Europe HORSE project. **CNIT leads the exploitation effort**, leveraging the consortium's combined expertise in AI-driven cybersecurity, network automation and Digital Twin technologies etc. The HORSE Platform benefits from the strong technical foundation developed during the project and from the close collaboration of partners such as research institutions, system integrators, and industrial stakeholders who contributed to the validation of the early prototypes.

Since the TRL of this KER at the end of the project will be 4-5, **the primary focus for HORSE platform is further research, development and technical consolidation**. In the short term, the goal is to advance the platform from its current project-level maturity toward a more robust, engineered, and integrable version, strengthening architecture components, expanding the mitigation-action database, improving ML models, and enhancing interoperability across physical and virtual infrastructures. In long-term, the consortium aims to position HORSE as a reference open-source framework for predictive and automated security in future 5G/6G networks, enabling continuous innovation, supporting additional research projects, and serving as a foundation for new collaborations with telecom operators, cybersecurity enterprises and standardisation bodies.

Objectives:

- Short-term (0-3 years after the end of the project):
  - Search for funding opportunities in order to support the operative plan.
  - Engineering of the HORSE architecture into a stable open-source release.
  - Strengthening internal interfaces and extending the mitigation-action database.
  - Increasing the technical maturity of the HORSE platform's subcomponents.
  - Start establishing partnerships with system integrators and telco enterprises in order to find early adopters.
  - Dissemination activities through conferences, publications, workshops etc. in order to continue building a community around the platform.
  - Discuss and finalise the IPR strategy and a JOA of the platform with all consortium partners.
  - Finalisation of a fully functional prototype (TRL 6-7).

- Long-term (3+ years after the end of the project):
  - Integration with physical and virtual infrastructures of early adopters.
  - Continuous refinement of all HORSE platform mechanisms.
  - Expansion of supported use cases aligned with early 6G deployments.
  - Establish the HORSE Platform as a reference open-source framework for predictive, automated, and AI-driven cybersecurity in 6G networks.
  - Contribute to standardisation activities (e.g., 3GPP, ETSI, ITU-T, SNS-JU) to align the platform with emerging 6G security requirements.
  - Begin preparatory steps toward market entry, including: evaluating potential application domains where HORSE could reach operational validation, developing integration pathways with industrial partners and a finalization of an MVP.

Strengths and Success Factors of CNIT:

- Strong Academic Network
  - Consortium of major Italian universities, giving it a broad scientific base.
  - Access to diverse, high-level expertise across all fields of telecommunications and ICT.
  - Facilitates interdisciplinary research and multi-university collaboration.

- High Research Quality & Innovation Capacity
  - Strong track record in national and EU-funded projects (Horizon, PNRR, ESA, etc.).

  - Recognized excellence in areas like 5G/6G, photonics, optical networks, cybersecurity, and AI for communications.
  - Ability to produce high-impact scientific publications and patents.

- Integration With Industry & Public Institutions
  - Long-standing collaborations with industry leaders (telecom operators, equipment vendors, technology companies).
  - Participation in strategic national and European telecom initiatives and standardization bodies.
  - Effective technology transfer capabilities.

- Advanced Laboratories & Research Facilities
  - Access to specialized labs across member universities.
  - Distributed infrastructure that supports experimentation in cutting-edge telecom technologies.

- Reputation & Institutional Credibility
  - Established over 30 years ago with solid national and international recognition.
  - Trusted partner for government agencies, regulators, and EU research frameworks.
  - Known for its contribution to innovation in Italian telecommunications.

- Talent Development
  - Strong role in educating and training PhD students, researchers, and engineers.
  - Facilitates mobility programs, networking, and early-career research opportunities.

Weaknesses and challenges of CNIT:

- Organizational Complexity
  - Distributed, multi-university structure makes coordination and decision-making more difficult.
  - Potential bureaucratic delays due to multiple administrative layers.

- Competition for Funding
  - Increasing competition from independent research centers, private R&D labs, and EU consortia.
  - Dependence on external project funding introduces financial uncertainty.

- Resource Fragmentation
  - Research infrastructures and teams spread across universities can lead to duplication of efforts.
  - Difficulty in centralizing equipment investments and maintaining shared platforms.

- Limited Autonomy/Governance Constraints
  - Being tied to university structures sometimes limits operational agility.
  - Variation in priorities, capabilities, and funding models across member institutions.

- Attracting and Retaining Talent
  - Competition from private telecom and tech companies offering higher salaries.
  - Challenge to retain young researchers once they complete PhD or project-based positions.

- Need for Greater International Visibility
  - Strong national presence, but must continue to strengthen global partnerships to match top-tier international telecom research centers.
  - Requirement to compete with larger, well-funded international institutions in 6G and emerging ICT fields.

- Rapid Technological Evolution
  - Must continuously invest to stay aligned with fast-paced telecom innovation (e.g., 6G, quantum communications, AI-driven networks).

- Risk of lagging behind if funding or infrastructure updates are delayed.

3. The product/service

The HORSE platform is a complete set of features and functionalities towards a secure 6G system orchestration. The project envisions two main "go-to-market" deployment modes: (i) **HORSE-as-a-Service**: an intermediary (e.g. an SME) offers HORSE's functionalities to end users — effectively providing secure, intelligent 6G-ready services, (ii) **on-Premises HORSE Deployment**: organizations (enterprises, operators) deploy HORSE within their infrastructure to manage their 6G (or 6G-ready) networks, make decisions, orchestrate resources, ensure security, etc.

Key components include:

- **Threat detection and Mitigation Engine:** Tool responsible for detecting threats in a predictive form, thus proactively acting towards removing or in the worst case mitigating the impact of the foreseen threat.

- **Network Digital Twin (NDT):** NDT is a software module that provides an accurate replica of the network infrastructure which is fed with the real time data. The NDT is capable of providing a detailed vision of the state of the network and predict short time future, including security threats and anomalies.

- **Distributed AI Engine for Services Preassessment:** Set of functionalities (Sandboxing, AI contextual models, etc.) to be used to replicate the entire 6G landscape in order to conduct a preliminary performance assessment of the tentative orchestration strategies to be deployed, aimed at ensuring that all deployed services run in a secure, distributed and optimized environment.

- **Intent-based Secure cross – Domain Orchestrator:** Includes a set of tools to logically and physically interact with the infrastructure elements to provide a secure cross-domain orchestration. The interaction will be handled through a proper mapping of high-level intents into security workflows able to react to security threats and vulnerabilities.

- **End to end Proactive Secure Connectivity Manager (ePEM):** ePEM plays a pivotal role in the HORSE security infrastructure. HORSE represents a cutting-edge security infrastructure designed to safeguard complex, distributed, and heterogeneous systems. In this intricate environment, the ePEM serves as a central architectural element, orchestrating actions and providing observability over the various components that constitute the end-to-end services secured within the HORSE security perimeter

- **Smart Monitoring (SM):** Responsible for the collection of data from all various and diverse domain resources, as well as data related to the usage of the resources involved in the lifecycle management.

- **Compliance Assessment (CAS):** CAS can make sure that every mitigation action that will take place will be compliant to regulations. It also provides an interface for users to check the history of the assessments that took place and their result.

- **Intent-based Interface (IBI):** The HORSE Intent-Based Interface is responsible for mapping high-level intents from a user, received as structured text or through a dedicated API, and further mapping those intents into use requirements. The requirements are then used to propose a list of deployable network policies that can mitigate attacks happening in the network or prevent future attacks. The policies are sent to a lower-level controller for deployment and enforcement in the network elements.

- **Early Modelling (EM):** A framework for the modeling of vulnerabilities, threats, attacks, proactive actions, mitigations, and estimated impacts.

- **Pre-processing:** A middleware solution designed to orchestrate and bolster a wide array of data sources, ranging in scale and structure, within cohesive and scalable data environments.

- **Policy Translator (PT):** Translator between IBI, EM and UMU orchestrator (Bastion) to execute intents on IA-NDT pods. Allows actions (QoS, Filtering) to be applied and/or metrics queries (monitor) to be performed.

- **Common Knowledge Base (CKB):** The CKB is an intelligent system that harnesses the power of multiple state-of-the-art LLMs to dynamically enrich a cybersecurity knowledge base, going beyond traditional static knowledge bases.

- **Policies and Data Governance (PAG):** A module which encrypts and anonymises the collected datasets, and logs the operations performed on the datasets of interest.

The HORSE platform is currently at TRL 4-5, having been demonstrated in an operational environment at the pilot sites. The platform as well as the majority of the core components are not yet completely developed. The consortium anticipates **a time-to-market of 3-5 years** to move from the project prototype to a fully marketed solution.

4. The market

The HORSE Platform targets the **Cybersecurity** and more specifically the **Network Security** market, a rapidly expanding sector that support the protection of digital infrastructures, critical facilities, cloud ecosystems, and connected operational environments. As organisations increasingly rely on real-time data flows, distributed systems, and automation, the need for intelligent, AI-driven monitoring and threat-mitigation solutions (such as those implemented within HORSE) has become essential.

According to recent estimates by [1], the global cybersecurity market is projected to grow from USD 227.59 billion in 2025 to USD 351.92 billion by 2030, corresponding to a Compound Annual Growth Rate (CAGR) of approximately 9.1% during the forecast period. Its growth is driven by a surge in targeted cyberattacks, increasing sophistication of threats, and the expanding need for organizations to protect critical business assets, data, and infrastructure against a complex and evolving threat landscape.

The Network Security Market is forecast to grow from USD 78.2 billion in 2024 to USD 111.0 billion by 2029, reflecting a CAGR of 7.2%. Its growth is driven by the rising number of DDos and zero-day attacks, adoption of cloud and hybrid environments and increasing number of connected devices [2].

The sector is characterised by a combination of mature foundational technologies and rapid innovation cycles, largely driven by AI and machine learning, digital twins, automation, and contextualised threat intelligence. AI-enabled intrusion detection and response systems are becoming essential for handling complex, multi-vector attacks at scale, especially within dynamic 5G/6G environments [3]. Digital twin technologies are also increasingly adopted to support resilience, enabling simulation, prediction, and validation of threat behaviours within virtual replicas of network infrastructures [4].

Despite strong market potential, the cybersecurity and network security sectors remain highly competitive, dominated by well-established global players such as Cisco, Palo Alto Networks, and Fortinet, alongside a growing ecosystem of specialised SMEs offering niche or innovative solutions [1]. Barriers to entry include the need for strong credibility and trust, compliance with multiple regulatory frameworks, substantial R&D investment, and the requirement for seamless integration into heterogeneous infrastructures. Nevertheless, new entrants can compete effectively by offering differentiated, high-value innovation—particularly in areas such as autonomous security management, cross-domain observability, and next-generation resilience technologies reinforced by AI and digital twins [5].

Political and regulatory developments significantly influence the sector's evolution. In the European Union, policies such as the NIS2 Directive [6], and the GDPR [7] impose stringent requirements for cybersecurity readiness, incident reporting, supply-chain security, and risk management across essential and important entities.

The main target customer segments for the HORSE platform include telecommunication operators, infrastructure providers, service developers, and network managers within telecom enterprises which operate highly complex, distributed network environments and are responsible for ensuring secure, high-performance 6G services and applications.

Their core needs revolve around achieving accurate threat detection, predictive attack management, real-time mitigation and full lifecycle security automation. They also increasingly require the capability to anticipate potential attack impacts in advance, manage security policies across multiple domains, and ensure the robustness of their network infrastructure.

Thus, by offering an intelligent, AI-powered framework that addresses both established and emerging security threats, the HORSE platform can be aligned with the evolving demands of future stakeholders, including industry, public authorities, and service providers. While 5G/6G networks promise unprecedented levels of connectivity, speed, and reliability, they also introduce a twofold challenge: the persistence of conventional cyber threats such as DDoS attacks, alongside new vulnerabilities arising from the unique architectural features of next-generation networks. Within this rapidly changing environment, the HORSE platform may be a strong candidate tailored to meet these complex security needs as it leverages an extensive range of AI capabilities, integrating state-of-the-art technologies into a unified architecture that includes parallel machine learning algorithms, dedicated digital twins, intent-based recommendation mechanisms, and fully automated mitigation systems.

Beyond its initial focus on the cybersecurity and network security domains, the HORSE platform presents strong potential for expansion into a wider range of vertical market areas where secure, resilient, and intelligent networked infrastructures are mission-critical. Due to its modular architecture, HORSE platform can be deployed in any environment that requires secure interconnection of heterogeneous systems, real-time monitoring, and automated threat mitigation.

One prominent expansion domain is healthcare, where hospitals, medical facilities, and healthcare providers increasingly rely on interconnected digital infrastructures, medical IoT devices, cloud platforms, and real-time data exchange. In such environments, HORSE could support the secure orchestration of distributed systems, protect sensitive patient data, ensure integrity and availability of critical services, and enable proactive detection of cyber threats that could compromise medical operations.

Another promising future market area is smart grids and energy infrastructures, where secure communication, resilience, and real-time situational awareness are fundamental requirements. Power generation units, substations, grid management platforms, and energy distribution networks operate as cyber-physical systems with strict reliability and safety constraints. In this context, the predictive security, impact analysis, and automated response mechanisms of HORSE could be leveraged to protect critical energy infrastructures from cyber threats and reduce outage risks. Similar opportunities may also emerge in smart cities, industrial automation, transportation systems, and large-scale IoT ecosystems, all of which depend on secure, high-performance, and resilient network connectivity.

SWOT analysis for the HORSE platform

Internal factors	
Strengths	**Weaknesses**

• Real time protection
• Quick identification and classification of potential security risks
• Additional layers of security providing:
  ○ Prediction and/or early detection of possible attack pathways,
  ○ proactive identification of vulnerabilities, and
  ○ evaluation on the effect of security events by simulating different network settings, configurations and attack scenarios
  ○ Streamlined configuration
  ○ Simplified Management
	• Dependence on a (limited size) mitigation action database
	• The list of intents is limited and only covers a small spectrum of the current 5G and beyond-5G threat landscape
	• The HORSE platform requires connectors to the different network infrastructure
	• The HORSE platform can increase the complexity of the system
	• Potential modification of the attack surface of the system
	• There is still a probability of wrong detection

○ The platform strictly complies with regulations and policies ○ Service optimisation via distributed resource allocation ○ Provision of coordination and observability of different components, securing end to end services deployed in complex, distributed and heterogeneous systems ○ Management of network and computing part of the infrastructure ○ Fast and early detection of new form of attacks ○ Fully compatible with 5G/6G infrastructure ○ mitigation of threats in networks using a declarative language ○ pre-assess the effects of mitigation actions using a network digital twin, allowing better decisions about the actions that should be activated/implemented in the network. ○ modelling of threats, vulnerabilities, attacks, preventive actions and mitigation strategies, thereby enhancing threat prediction and the assessment of preventive measures within the context of NDTs. ○ consistently and securely access harmonized data on attacks and countermeasures via REST APIs. ○ encryption and anonymisation of collected datasets allow the entire platform to guarantee high-level data governance and compliance with strict regulations (like GDPR) • Scalable and agile	
External factors	
Opportunities	**Threats**
• Rapid evolution of 5G/6G ecosystems • Increasing interest in more sophisticated network security technologies like HORSE • Rising demand for advanced threat detection and prevention	• Competition from major telecom vendors • Emergence of more sophisticated cyberattacks • Fast-changing 5G/6G standards and regulatory uncertainty • Limited adoption potential

Strengths

The HORSE platform demonstrates strong capabilities in real-time protection and rapid identification of security threats, enabling timely detection and classification of potential risks in complex network environments. Its advanced security mechanisms support early prediction of attack pathways, proactive vulnerability identification, and impact evaluation of security events through simulation of different network configurations and attack scenarios using Network Digital Twins (NDTs). This allows operators to assess mitigation actions before deployment and make informed decisions.

Additionally, the platform offers streamlined configuration and simplified management, reducing operational overhead while maintaining high security standards. HORSE provides end-to-end coordination, observability, and management of network and computing infrastructure, supporting secure service deployment across heterogeneous and distributed systems. Its compatibility with 5G/6G infrastructures, use of declarative languages for threat mitigation, and secure access to harmonised threat intelligence via REST APIs further enhance its scalability, agility, and interoperability. Strong data governance is ensured through encryption and anonymisation mechanisms, guaranteeing compliance with strict regulatory frameworks such as GDPR.

Weaknesses

One of the main weaknesses of the HORSE platform is its dependence on a mitigation action database of limited size, which may constrain the coverage of potential countermeasures. Similarly, the current set of intents addresses only a subset of the evolving 5G and beyond-5G threat landscape, limiting flexibility against emerging attack patterns.

The platform also requires connectors to diverse network infrastructures, which can increase integration effort and deployment complexity. As a result, HORSE may introduce additional system complexity and, in some cases, modify the attack surface of the protected infrastructure. Finally, as with any advanced detection system, there remains a residual probability of false positives or false negatives, which may affect operational trust during early adoption phases.

Opportunities

The rapid evolution of 5G and 6G ecosystems creates significant opportunities for advanced, AI-driven security solutions such as HORSE. As network architectures become more distributed, virtualised, and software-defined, the demand for automated, proactive, and predictive security mechanisms is steadily increasing.

At the same time, there is growing market interest in sophisticated threat detection, prevention, and mitigation technologies, driven by stricter regulatory requirements and the increasing cost of cyber incidents. HORSE is well positioned to capitalise on this trend by offering an integrated, future-proof security framework that supports next-generation network infrastructures.

Threats

The presence of large telecom vendors in the network security market represents a significant competitive threat, as these actors benefit from established customer bases, strong brand recognition, and tightly integrated end-to-end solutions. To mitigate this risk, the HORSE platform focuses on differentiation through advanced capabilities such as Network Digital Twin–based simulations, declarative security management etc.

The continuous evolution of cyberattacks poses a persistent threat, as new attack techniques may exceed the detection capabilities of static or rule-based security mechanisms. HORSE may address the challenge by enabling continuous evolution of its threat models and mitigation strategies, supported by proactive vulnerability assessment and predictive analysis.

The rapid evolution of 5G and upcoming 6G standards, combined with regulatory uncertainty across regions, may affect long-term compatibility and compliance of security solutions. HORSE can mitigate the threat through a modular, standards-aware architecture that allows components to be updated or replaced with minimal impact on the overall system.

Limited adoption may arise due to perceived complexity, integration effort, or concerns related to deploying advanced security mechanisms in operational environments. However, this risk is mitigated by the high replicability and adaptability of the HORSE platform across multiple application domains.

Thanks to its modular and technology-agnostic architecture, HORSE can be adapted to any sector requiring secure, resilient, and intelligent networked infrastructures, beyond its initial focus on 5G/6G and telecommunications environments.

5. The business model and marketing strategy

The primary strategic focus of the HORSE Platform after the project's completion will be **continued research and development**, aiming to further mature, validate, and technically enhance the solution before any large-scale market-oriented activity takes place. During this phase, early interactions with potential adopters (such as system integrators and telecommunications stakeholders) may begin, but always with the aim of supporting further R&D rather than immediate commercialization.

In parallel, the HORSE platform is expected to gradually build its pathway toward future monetization strategies. Given the technology's nature and the open-source release plan, revenues might emerge primarily from service-based models, such as consultancy, integration support, training, and customized deployments.

The marketing strategy for HORSE will rely on the two envisioned deployment modes, which may accommodate both early adopters and larger industrial players. In the **HORSE-as-a-Service** model, an intermediary organization may operate HORSE in the cloud and offer secure, intelligent, 6G-ready functionalities to users who do not have the internal capacity or resources to manage security orchestration systems themselves. In contrast, the **on-premises deployment** modality is aimed at organizations (including telecom operators and infrastructure providers) that may require full internal control of the platform for managing sensitive 6G or 6G-ready environments.

In the medium-to-long term, HORSE's marketing strategy may rely on a combination of open-source visibility and targeted engagement activities. Outreach may include publishing scientific results, releasing code through platforms such as GitHub, and participating in major networking and cybersecurity conferences, webinars, and specialized events. Promotional investment may remain modest during the R&D-centric phase, primarily covering the continuous community building around the platform, while later stages might involve more structured marketing actions once the platform reaches higher TRLs.

Pricing strategies will likely follow **a service-oriented model**, where consultancy, customization, and support services may be priced based on the complexity of integrations and the level of operational involvement required. For deployments involving on-premises installations, tailored pricing schemes might be introduced (potentially including annual maintenance agreements, security lifecycle management services, or specialised feature extensions). For HORSE-aaS, subscription-based models could be explored, although only after the platform reaches the necessary maturity for stable operation.

6. The Team and management structure

The HORSE Platform will be further developed, maintained and managed by a highly qualified research-driven team within CNIT, supported by the wider HORSE consortium. The core internal CNIT team involved in the HORSE Platform includes:

- Fabrizio Granelli, Full Professor in Networking, coordinator of the project
- Raffaele Bolla, Full Professor in Networking, the Director of the CNIT S2N Lab (in Genoa)
- Roberto Bruschi, Full Professor, responsible for CNIT S2N Lab testbed (in Genoa)
- Alessandro Carrega, Researcher on SDN networks
- Rawlings Ntassah, Researcher on Software Networks
- Samia Saidane, Doctoral Researcher on Cybersecurity

Marketing, fundraising, IP management and exploitation will be handled by CNIT in collaboration with University of Trento (the CNIT Research Unit of the HORSE Project Coordinator):

- Paola Magri, CNIT Staff, support to exploitation
- Giuseppe Caputo, U. Trento Staff, IP management and fundraising
- Vanessa Ravagni, U. Trento Staff, fundraising
- Mirella Erario, U. Trento Staff, marketing and exploitation

The functional responsibilities within the HORSE technical, exploitation and business framework are currently structured as follows:

- **Scientific and Technical Coordination:** Will be led by the Project Coordinator, in order to achieve alignment of R&D activities and technical roadmap definition.
- **Architecture Design and Integration:** Can be managed by senior researchers and lab directors, responsible for system-level integration, interoperability and testbed-driven validation.
- **Cybersecurity and ML Research:** Will be conducted by specialized researchers and doctoral candidates, focusing on threat detection, predictive security mechanisms, anomaly detection etc.
- **Testbed Operation and Validation:** May be coordinated within the CNIT S2N Laboratory, supporting realistic experimentation and system evaluation.
- **Dissemination and Knowledge Transfer:** Can be managed through scientific publications, conference participation, and technical workshops.
- **Marketing:** Will be coordinated by CNIT and will focus on early-stage customer development and stakeholder engagement activities, including interaction with potential stakeholders (e.g. network operators, system integrators, research infrastructures), collection of feedback validation of technical assumptions, and communication of the HORSE Platform through scientific dissemination channels, technical workshops, and targeted outreach activities.
- **Fund raising:** Can be managed by CNIT and will focus on the identification, preparation, and submission of follow-up funding proposals to support the next development phases of the HORSE Platform, with particular emphasis on EU funding instruments.

Moreover, at the current stage, the HORSE Platform is intentionally research-oriented, and therefore certain roles typically found in commercial organisations (such as sales management, large-scale operations and commercial product ownership) are not yet established.

7. The operative plan

Following project completion, the primary collective focus of the consortium **will be further R&D, with the objective of increasing the platform's maturity and readiness for real-world deployment.** HORSE is a technically complex system composed of multiple interoperable components; therefore, the R&D process will operate on two parallel axes:

1. Consortium-wide activities in the HORSE platform

The consortium will continue joint activities aimed at strengthening integration, security orchestration, and performance. These activities may include:

- Search for funding in order to support the operation roadmap (will start at 1 month after the project completion)
- Further engineering of the HORSE platform architecture (will start at 1 month after the end of the project). More specifically:
  - Interfacing with physical infrastructure
  - Securing internal interfaces among the subcomponents
  - Increasing the technical maturity of each HORSE subcomponent
- Discussions for the final joint business plan, JOA and IPR strategy among the consortium partners (will start at 6 months after the end of the project)
- Dissemination activities form all consortium partners in order to continue the community building around the platform (IEEE, ICC, NFVSDN conference etc.) (will start at 6 months after the end of the project)

- Customer development and customer validation activities such as identification of early adopters, validation of use cases, refinement of platform's requirements etc. without assuming immediate market entry (will start at 8 months after the end of the project)

2. Individual partner's R&D activities for their subcomponents

Thanks to the modularity of the HORSE platform, each partner can independently increase the maturity of its own HORSE platform building block. As individual components mature during the time, the platform TRL will rise accordingly, since HORSE platform depends on the collective performance of its constituent modules.

Briefly, for the key components referred to Chapter 3 the further R&D activities in order **to reach TRL 6-7** will include:

- For **Threat detection and Mitigation Engine** (will start in 3 months after the end of the project):
  - Continuous integration, testing and validation of the technology according to the platform's stakeholders' requirements.

- For **Network Digital Twin** (will start in 3 months after the end of the project):
  - Code optimization and software engineering
  - Additional development to increase self-configuring capabilities
  - Support for new security threats
  - Automation deployment (e.g. automatic deployment/configuration of topology and attacks)
  - Additional development of interfaces to networking hardware devices

- For **Distributed AI Engine for Services Preassessment** (will start in 6 months after the project completion):
  - Integration of more advanced ML approaches according to the analysis of stakeholder's requirements of the HORSE platform
  - Enforcement of more robust security mechanisms

- For **Intent-based Secure cross – Domain Orchestrator** (will start in 1 month after the end of the project):
  - Quality assurance and quality testing in multiple end-to-end tests in order to further validate the component into different environments.
  - Optimisation of the deployment pipelines in order to have seamless deployment in new use cases.

- For **End-to-end Proactive Secure Connectivity Manager** (will start in 3 months after the end of the project):
  - To develop a blueprint dependency matrix in order to simplify the resolution of possible security problems that can arise in some services provided by the ePEM.
  - Integrate some AI mechanisms in order to automatically create the blueprint dependency matrix checking the different available blueprints.

- For **Smart Monitoring** (will start in 2 months after the project end):
  - Adjust the SM into STS tools for better knowledge and testing
  - Research on other possible data types that SM can digest and transform to JSON
  - Adding other use cases of SM (research on other possible use cases on different disciplines for further validation)

- For **Compliance Assessment** (will start in 2 months after the project end):
  - Incorporate GDPR, NIS2, ENISA and other directives and regulations
  - Expand the feedback mechanism on partial compliance

- For **Intent-based Interface** (they will start in 1 month after the end of the project):
  - Expanding collaboration with industry partners to adapt the component to a broader range of attacks, intents, and mitigation actions

  - Alignment of IBI's interfaces with industry-standard solutions in order to adapt its logic to a broader security landscape

- For **Early Modelling** (they will start in 3 months after the project end):
  - Integration of the EM tool into ongoing 5G/6G security initiatives to validate its performance in attack surface identification, threat prediction, and pre-assessment workflows.
  - Consider other use cases for further validation (e.g. in healthcare or in different types of attacks).

- For **Pre-processing** (will start in 1 month after the end of the project):
  - Quality assurance and quality testing in multiple end-to-end tests in order to further validate the component into different environments.
  - Addition of a load management system in order to handle data in parallel.

- For **Policy Translator** (will start in 1 month after the end of the project):
  - Define and enforce strict validation for both incoming and outgoing payloads (e.g., JSON Schema and/or OpenAPI), add regression tests (valid/invalid cases), and standardize error responses to avoid silent translation failures.
  - Add token-based authentication (e.g., Bearer/API key via environment variables), minimal audit logging (caller, timestamp, outcome), and clear operational documentation for credentials/configuration handling.
  - Complete end-to-end deployment integration (configuration, networking, runtime parameters) and validate stable operation in an IA-NDT-like setup.

- For **Common Knowledge Base** (will start in 2 months after the end of the project):
  - **Commercial Environment Validation:** Evolving from the initial validation Validation of the CKB performance using real threat data streams within the Orchestra Cities ecosystem. This serves as the operational environment demonstration (TRL 7) to verify the component's scalability within a commercial IoT platform.
  - **Service Hardening & Integration:** Refactoring the Attack/Mitigation Service from an R&D prototype into a production-grade security module. This includes implementing industry-standard API security and error handling to ensure seamless interoperability with the Orchestra Cities infrastructure.
  - **DevSecOps Pipeline:** Establishing a CI/CD pipeline with automated security scanning (SAST/DAST) to support the continuous delivery of these security features into our commercial portfolio

- For **Policies and Data Governance** (will start in 1 month after the end of the project):
  - Harden the interfaces to ensure robust, high-volume data collection and secure data exchange with other components (like the Smart Monitoring component)
  - Conduct rigorous stress testing (simulating high-density data traffic typical of 5G/6G applications).
  - Demonstrate the core functions—data encryption, anonymisation, and logging—at target performance levels (e.g., verifying negligible latency addition by the PAG component)
  - Run the integrated PAG within the relevant 5G/6G testbed. Gather performance and security metrics, document the stability of the module.

R&D progress may require the use of testbeds, simulation environments, and infrastructure for integration testing and may include:

- cloud-based environments for orchestration testing
- virtualised network slices for evaluating HORSE-as-a-Service
- controlled on-premise testbeds for evaluating HORSE in operator-like conditions
- computational facilities for ML model training and large-scale simulations
- digital twin environments for predictive security analysis

As a final comment, a strategic exploitation decision milestone is foreseen once the HORSE Platform reaches TRL 6–7 and completes initial large-scale validation activities. At this stage, two alternative

exploitation paths will be evaluated: (i) the creation of a dedicated **spin-off** entity, or (ii) **the licensing** of the HORSE technology to an experienced system integrator already serving the telecom market. The decision will be based on technical maturity, validation results, market interest and the availability of industrial partners.

8. Financials

As mentioned in the previous chapters, the primary focus of the HORSE platform will be further R&D in order to reach TRL 6-7. So, the costs for the activities mentioned in Chapter 7 for reaching a higher level of maturity and the other activities may be:

For CNIT:

- **R&D costs** (such as maintenance, engineering, production): €15,000 – 30,000
- **Dissemination costs**: around €2,000 per conference
- **Licensing costs** (either from the other consortium partners or third parties): €5,000 – 10,000
- **Infrastructure maintenance costs**: €3,000 – 5,000
- **Project management costs**: €40,000 – 60,000

For the further R&D activities of each key component:

- For **Threat detection and Mitigation Engine:** €0 (the circuit has reached its full maturity for the HORSE platform, the new round of costs will be calculated when the collection of stakeholders' requirements is finished)
- For **Network Digital Twin (NDT):** €35,000 – 65,000
- For **Distributed AI Engine for Services Preassessment:** €15,000 – 25,000
- For **Intent-based Secure cross – Domain Orchestrator:** €35,000 – 50,000
- For **End-to-end Proactive Secure Connectivity Manager (ePEM):** €20,000 – 50,000 (ask Alex)
- For **Smart Monitoring (SM):** €40,000 – 80,000
- For **Compliance Assessment (CAS):** €10,000 – 20,000
- For **Intent-based Interface (IBI):** €45,000 – 70,000
- For **Early Modelling (EM):** €45,000 – 55,000
- For **Pre-processing:** €25,000 – 35,000
- For **Policy Translator:** €23,000 – 37,000
- For **Common Knowledge Base**: €140,000 – 160,000
- For **Policies and Data Governance:** €25,000 – 35,000

Apart from the R&D activities, the consortium estimates a range for other costs for the HORSE platform over the full duration of the next development phase. Briefly they will be:

- **Dissemination, communication and marketing costs** (such as website and social media creation and management, drafting publications, organisation of webinars and workshops, participation to relevant conferences and events, promotional material, promotional campaign for stakeholders and customer engagement): 350,000 – 600,000
- **Infrastructure maintenance:** €200,000 – 400,000
- **Legal costs:** €100,000 – 200,000

The estimated horizontal operational and management costs for CNIT (including R&D coordination, system engineering, production support, project management, dissemination and comminication activities, licensing, and infrastructure maintenance) range between €65,000 and €107,000 (with participation in one dissemination event).

In parallel, the further research and development of the core technological components of the HORSE Platform requires an estimated investment between €428,000 and €672,000. The Threat Detection and Mitigation Engine is considered technically mature at this stage and therefore does not introduce additional R&D costs in the current phase.

Overall, the total estimated R&D and supporting cost envelope for the next development phase of the HORSE Platform is expected to range between approximately €493,000 and €779,000. Furthermore, the total summary of the R&D and other costs **will be around 1.2 – 2 million euros**.

Finally, it is worth to note that, at this stage, no revenue projections are provided, as the platform remains in a research-driven development phase and any commercial assumptions would be premature and not evidence-based.

9. The resources

The implementation of the HORSE Platform in the market will primarily rely on a phased investment plan, strongly focused on further research and development, technology maturation, and community-driven validation, before moving to large-scale commercial deployment. During the initial operational phase, financial resources may mainly be directed towards enhancing the technical maturity (TRL) of the platform, strengthening its core security, orchestration and automation capabilities.

Funding to support the above activities may be obtained from a combination of sources, including internal organisational funds, participation in additional national and European research and innovation projects, and (at later stages) potential private investments or strategic partnerships with industrial stakeholders. The project partners may also explore collaborations with system integrators, telecom infrastructure providers, and cybersecurity-driven enterprises, which could contribute to co-funded development actions, joint pilots, or technology validation activities.

One promising funding opportunity targeted to support the transition of the HORSE Platform from TRL 4-5 to TRL 6 is the **EIC Transition programme [8]**, which is specifically designed to mature promising results from EU-funded research projects towards market readiness. A potential target within the JU-SNS would be JU-SNS-2026-STREAM-B-01, particularly on what relates to the security concepts.

The timing of the required financial resources is expected to follow a gradual multi-year approach. In the short term, resources will mainly support engineering activities, architectural refinement, security hardening, integration of sub-components, and dissemination actions aimed at strengthening the user and developer community around HORSE. In the long term, additional investments may be required for large-scale validation, pilot deployments, compliance activities, and potential pre-commercial demonstrations. Only at a more advanced stage, when the platform reaches higher TRL levels, external private funding or investor-driven resources might be considered to accelerate market entry.

Connection between HORSE and MARE

The exploitation and further development strategy of some HORSE results is supported by continuity actions that extend beyond the lifetime of the HORSE project. In this context, the project MARE represents a key follow-up initiative that builds upon the technical foundations, architectural principles, and experimental outcomes achieved within HORSE.

MARE is a HORIZON EUROPE project, started in January 2025, funded in the third SNS-JU call focused on enhancing the security and resilience of future 6G networks by introducing a novel, open, modular and programmable Security Plane that can operate transparently across multiple domains and stakeholders. Its objectives include defining enriched security building blocks (known as DOTs), combining them into programmable security services, and developing a smart pre-assessment environment with simulation and emulation tools to analyse and validate security functions and strategies for 6G systems. MARE also aims to implement a systematic attack modelling reference framework to identify and categorise emerging threats in the evolving 6G ecosystem, with demonstrations planned in multiple proof-of-concept scenarios to validate its security solutions within compliant 6G architectural concepts.

The work to be done in MARE is strongly leveraging HORSE project ideas and outcomes. Indeed, both projects share the same objective, namely to guarantee a secure 6G services deployment. Considering this common target, HORSE set the foundations for a proactive approach based on several innovations, including aspects related to attacks detection and prediction based on a specific ML training process, an intent-based approach to make users aware on the different internal processes as well as to automatize the decision-making processes, and the pre-assessment strategy where any action is to be tested in a Sandbox context before being deployed. Thus, many architectural components, such as the IBI, EM, DEME or the SAN will act as the seed for MARE to successfully develop the proposed softwerised solution. MARE extends the work in HORSE through a softwerised approach, that based on a composing and orchestrator functionality may dynamically generate the proper Security Function to manage any cyberattack to come up. This effort and the HORSE legacy may be summarized in three key points. First, the proactive approach supported by a predictive strategy where attacks are either

predicted or early detected. This approach is also easing the management of new attacks where no actions either preventive or mitigation, have been defined so far. Second, the pre-assessment strategy defined in HORSE is extended in MARE with the NOWIT concept (not without being tested) where both attacks and mitigation/preventive action are analysed. Consequently, the proposed emulated environment is used to classify the impact an attack may have what would strongly contribute to define the action to be taken, as well as to analyse the impact a potential action would have on the infrastructure, to guarantee that no harmful actions will be deployed. This is particularly interesting considering that a proactive approach based on estimations is to be considered, so extremely sensible to prediction errors. Third, the intent-based approach that guarantees an open, extendable, and human-friendly approach to manage the decision-making process.

10. References (For Module D)

[1] "Cybersecurity Market Size, Share, Analysis | Growth & Forecast [2032]," MarketsandMarkets. Accessed: Dec. 09, 2025. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html

[2] MarketsandMarkets, "Network Security Market worth $111.0 billion by 2029 - Exclusive Report by MarketsandMarketsTM." Accessed: Dec. 09, 2025. [Online]. Available: https://www.prnewswire.com/news-releases/network-security-market-worth-111-0-billion-by-2029---exclusive-report-by-marketsandmarkets-302248853.html

[3] A. Thakkar and R. Lohiya, "A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions," Artif. Intell. Rev., vol. 55, Jan. 2022, doi: 10.1007/s10462-021-10037-9.

[4] B. Ghimire and D. B. Rawat, "Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things," IEEE Internet Things J., vol. 9, pp. 1–1, Jun. 2022, doi: 10.1109/JIOT.2022.3150363.

[5] A. Arulappan, J. Luzzi, R. Naha, and A. Mahanti, "SOK: A Holistic View of Cyberattacks Prediction with Digital Twins," Feb. 2024. doi: 10.1109/ic-ETITE58242.2024.10493514.

[6] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance), vol. 333. 2022. Accessed: Dec. 09, 2025. [Online]. Available: http://data.europa.eu/eli/dir/2022/2555/oj

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), vol. 119. 2016. Accessed: Dec. 09, 2025. [Online]. Available: http://data.europa.eu/eli/reg/2016/679/oj

[8] "EIC Transition - European Innovation Council - European Commission." Accessed: Dec. 15, 2025. [Online]. Available: https://eic.ec.europa.eu/eic-funding-opportunities/eic-transition_en

15 Appendix F – Letter of support

Trentino Digitale SpA

Via G. Gilli 2, 38121 Trento | +39 0461 800111
tndigit@tndigit.it | tndigit@pec.tndigit.it
www.trentinodigitale.it

Trento, November 28, 2025

Letter of Support

To whom it may concern,

On behalf of **Trentino Digitale S.p.A.**, I am pleased to express our strong interest in the continued development, exploitation, and future adoption of the **Network Digital Twin** technology created by **CNIT/University of Trento** within the **SNS JU Project HORSE**.

Trentino Digitale is committed to advancing secure, resilient, and intelligent digital infrastructures in the Trentino region and beyond. We recognize the significant innovation potential of the Network Digital Twin developed in HORSE—particularly its ability to **model complex network behaviour**, **predict emerging security threats**, and **enable proactive mitigation strategies**.

Given the increasing sophistication of cyber-attacks and the need for more autonomous network defence mechanisms, we believe this technology can play a key role in improving the robustness and reliability of critical digital services.

We are therefore interested in:

- **Collaborating with CNIT/University of Trento** and HORSE partners to further mature the Network Digital Twin beyond the project's lifetime.
- **Evaluating opportunities for integration** of the Digital Twin into our operational environments, especially in areas related to monitoring, situational awareness, and cybersecurity of regional infrastructures.
- **Contributing to pilot activities**, validation efforts, or joint initiatives aimed at transferring the technology toward real-world deployments and market adoption.
- **Exploring commercial and industrial exploitation opportunities** that may arise from the technology's evolution.

Trentino Digitale considers the outcomes of HORSE to be highly relevant for the European digital ecosystem, and we support efforts to bring the Network Digital Twin to higher TRLs and into practical use. We look forward to continued collaboration that may lead to concrete deployment scenarios benefiting public administrations, enterprises, and citizens.

Please consider this letter as a formal expression of our interest and support for the exploitation pathway of the Network Digital Twin technology.

Sincerely,

Kussai Shahin
Chief Executive Officer (CEO)
Trentino Digitale S.p.A.

Trentino Digitale SpA
DIRETTORE GENERALE
Kussai Shahin

16 Appendix G – Final standardisation activities

Q1 2025

Date	SDO / Project / Organization	Contribution / Activity	Comments	Status Update
5/01/25	IETF OPSAWG	Contribution	New version of the telemerry provenance I-D proposal: https://datatracker.ietf.org/doc/draft-lopez-opsawg-yang-provenance/	Ongoing
12/02/25	ETSI	Charter	Establishment of a new Technical Committee on Data Solutions (TC DATA)	Approved by ETSI Board
11/03/25	3GPP Plenary	Meeting	3GPP 6G Workshop. Specific mentions in the chair's summary to: * An upper layer on top of SBA: AI INTENT MANAGEMENT LAYER https://www.3gpp.org/ftp/workshop/2025-03-10_3GPP_6G_WS/Docs/6GWS-250243.zip	Proposals included in the chair summary

Q2 2025

Date	SDO / Project / Organization	Contribution / Activity	Comments	Status Update
15/04/25	ETSI TC DATA	Leadership	Appointment as TC DATA chair https://docbox.etsi.org/DATA/DATA/05-Contributions/2025/DATA(25)000004_DATA_01_-_Draft_Meeting_Report.docx	Approved
15/04/25	ETSI TC DATA	Leadership	Reflections on TC DATA initial steps https://docbox.etsi.org/DATA/DATA/05-Contributions/2025/DATA(25)000051_Chair_Perspectives_for_DATA_01.pptx	Presented
15/04/25	ETSI TC DATA	Contribution	Position statement on data activities related to next-generation networks https://docbox.etsi.org/DATA/DATA/05-Contributions/2025/DATA(25)000018_Discussion_paper_on_Sensing__AI_and_Trustworthy_data_in_mobi.docx	Presented
15/04/25	ETSI TC DATA	Contribution	Position statement and presentation on data governance and semantic interoperability https://docbox.etsi.org/DATA/DATA/05-Contributions/2025/DATA(25)000042r1_Position_Paper_on_Data_Governance_and_Semantic_Interopera	Presented

			bil.docx https://docbox.etsi.org/DATA/DATA/05-Contributions/2025/DATA(25)000046_A_Position_Statement_on__Data_Governance_and_Semantic_Intero.pptx	
15/04/25	ETSI TC DATA	Charter	New work-item on Smart contracts https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=74839	Approved
17/04/25	ETSI TC DATA	Charter	New work-item on Oracles for Smart Contracts executed in Electronic Ledgers https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=74879	Approved
17/04/25	ETSI TC DATA	Charter	New work-item on data quality metrics https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=74875	Approved
17/04/25	ETSI TC DATA	Charter	New work-item on Landscape of Relevant Standards and Technologies for Data https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=74880	Approved

17/04/25	ETSI TC DATA	Charter	Four new work-items on NGSI-LD evolution https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=74870 https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=74871 https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=74872 https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=74873	Approved
17/04/25	ETSI TC DATA	Contribution	TC DATA introduction at the 6GFORGE event https://telcoforge.com/agenda-6g-forge-2025/ https://telcoforge.com/speakers-6g-forge-2025/	Presented
23/04/25	ETSI ZSM	Leadership	Chair reflections on the next term for ZSM, considering alternatives and future structure: https://pad-public.etsi.org/p/ZSM30 https://docbox.etsi.org/ISG/ZSM/05-CONTRIBUTIONS/2025/ZSM(25)000080r2_Chairman_Perspective_-_ZSM_30.pptx https://docbox.etsi.org/ISG/ZSM/05-CONTRIBUTIONS/2025/ZSM(25)000082_ZS	Presented

			M_30_Meeting_Report.docx	
23/04/25	ETSI ZSM	PoC	PoC Proposal, accepted as ZSM PoC#15 https://pad-public.etsi.org/p/ZSM30 https://docbox.etsi.org/ISG/ZSM/05-CONTRIBUTIONS/2025/ZSM(25)000082_ZSM_30_Meeting_Report.docx https://docbox.etsi.org/ISG/ZSM/05-CONTRIBUTIONS/2025/ZSM(25)000055r2_PoC_Proposal__Security_Management_with_NDT_support.docx https://docbox.etsi.org/ISG/ZSM/05-CONTRIBUTIONS/2025/ZSM(25)000088_ZSM_PoC_Proposal_on_Security_Management_with_NDT_support_-_P.pptx https://zsmwiki.etsi.org/index.php?title=Ongoing_PoCs	Proposal approved and published by ZSM
24/04/25	ETSI ZSM	Contribution	Discussions on the trust concept, and the use of existing mechanisms, such as LoA (NFV-SEC007) and Trust Management Service (ZSM014) in ZSM017 https://pad-public.etsi.org/p/ZSM30	Ongoing

24/04/25	ETSI ZSM	Leadership	Joint session with CCSA TC17, exploring collaboration on aspects related to Autonomous Networks, NDTs, agents and LLMs https://docbox.etsi.org/ISG/ZSM/05-CONTRIBUTIONS/2025/ZSM(25)000029_ETSI_ZSM30_CCSA_TC7_workshop_planning.docx https://docbox.etsi.org/ISG/ZSM/05-CONTRIBUTIONS/2025/ZSM(25)000082_ZSM_30_Meeting_Report.docx	Presented
9/05/25	IETF OPSAWG	Contribution	YANG provenance draft adopted https://datatracker.ietf.org/doc/draft-ietf-opsawg-yang-provenance/	Adopted by the WG
24/06/25	ETSI ZSM	Contribution	Link to the work in NASR and WIMSE on geolocation and path property attestation for ZSM019: https://pad-public.etsi.org/p/ZSM31 https://docbox.etsi.org/ISG/ZSM/05-CONTRIBUTIONS/2025/ZSM(25)000018_ZSM019_Clause_7_1_Background.docx	Included in ZSM019
24/06/25	ETSI ZSM	Contribution	Discussion on identity management and access governance for ZSM019: https://pad-public.etsi.org/p/ZSM31 https://docbox.etsi.o	Included in ZSM019

			rg/ISG/ZSM/05-CONTRIBUTIONS/2025/ZSM(25)000111_ZSM19_Clause_6_2_.docx	
24/06/25	ETSI ZSM	Leadership	Reflections on the future of the group and discussion on the potential ZSM extension: https://pad-public.etsi.org/p/ZSM31 https://docbox.etsi.org/ISG/ZSM/05-CONTRIBUTIONS/2025/ZSM(25)000130_Chairman_Perspective_-_ZSM_31.pptx	Presented and discussed
25/06/25	ETSI ZSM	Contribution	Discussion on the capabilities required to address autonomy: https://pad-public.etsi.org/p/ZSM31 https://docbox.etsi.org/ISG/ZSM/05-CONTRIBUTIONS/2025/ZSM(25)000121_ZSM021_Clause_7_Potential_ZSM_Capabilities_to_support_autono.docx	Included in ZSM021

Q3 2025

Date	SDO / Project / Organization	Contribution / Activity	Comments	Status Update
2/07/25	IETF NMOP WG	Leadership	Appointment of the Knowledge Graph Design Team: https://mailarchive.ietf.org/arch/msg/nmop/Rx2KmaKcVzbs1KhWskvrCxeQ_ZE/	Communicated by the NMOP chair
2/07/25	ETSI TC DATA	Leadership	Proposal on the WG structure of TC DATA: https://docbox.etsi.org/DATA/DATA/05-Contributions/2025/DATA(25)002045_Guidelines_on_TC_DATA_WG_Structure.pptx	Presented and accepted
2/07/25	ETSI TC DATA	Charter	New work item on Ontology mechanisms in support of the European Data Act https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=75367	Approved
2/07/25	ETSI TC DATA	Charter	New work item on data catalogue mechanisms in support of the European Data Act https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=75368	Approved

2/07/25	ETSI TC DATA	Charter	New work item on SAREF on NGSI-LD https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=75351	Approved
19/07/25	IETF Hackathon	Contribution	Demonstrator of the reference implementation for YANG data provenance: https://www.ietf.org/archive/id/draft-ietf-opsawg-yang-provenance-01.html https://datatracker.ietf.org/meeting/123/materials/slides-123-hackathon-sessd-yang-provenance-02 https://wiki.ietf.org/en/meeting/123/hackathon	Presented and discussed
19/07/25	IETF Hackathon	Contribution	Demonstrator of the application of knowledge graphs to construct NDTs: https://datatracker.ietf.org/meeting/123/materials/slides-123-hackathon-sessd-mouseworld-knowledge-graphs-for-network-digital-twins-00 https://wiki.ietf.org/en/meeting/123/hackathon	Presented and discussed
19/07/25	IETF IVY	Contribution	New version of the Internet draft on entitlement modeling, presented at the IVY meeting: https://www.ietf.org/archive/id/draft-mcd-ivy-entitlement-inventory-02.html https://datatracker.ie	Presented and appointed for adoption

			tf.org/meeting/123/materials/slides-123-ivy-entitlement-inventory-01 https://datatracker.ietf.org/meeting/123/agenda	
20/07/25	IETF NETCONF	Contribution	New version of the Internet draft on configuration tracing appointed for WG lat call: https://datatracker.ietf.org/doc/draft-ietf-netconf-configuration-tracing/ https://www.ietf.org/archive/id/draft-ietf-netconf-configuration-tracing-05.html	Presented and going to last call
20/07/25	IETF NETCONF	Contribution	New version of the Internet draft on the YANG augment realationship: https://datatracker.ietf.org/doc/html/draft-ietf-netconf-yang-library-augmentedby-11 https://datatracker.ietf.org/meeting/123/materials/slides-123-netconf-augmented-by-addition-to-the-yang-library-00 https://datatracker.ietf.org/meeting/123/agenda	Presented and discussed
20/07/25	IETF NMOP	Presentation	Update on the use of knowledge graphs for network management: https://datatracker.ietf.org/meeting/123/materials/slides-123-nmop-knowledge-graph-update-00	Presented and discussed

			https://datatracker.ietf.org/meeting/123/agenda	
21/07/25	IETF NMRG	Contribution	New version of the Internet draft on NDT architecture: https://datatracker.ietf.org/doc/html/draft-irtf-nmrg-network-digital-twin-arch-11	Presented and discussed
21/07/25	IETF NMRG	Contribution	New Internet draft on the use of MCP for network management, presented at the NMRG meeting: https://datatracker.ietf.org/doc/html/draft-yang-nmrg-mcp-nm-00 https://datatracker.ietf.org/meeting/123/materials/slides-123-nmrg-applicability-of-mcp-on-network-management-00 https://datatracker.ietf.org/meeting/123/agenda	Presented and discussed
21/07/25	IETF NMRG	Contribution	New Internet draft on the applicability of A2A to network management: https://datatracker.ietf.org/doc/html/draft-yang-nmrg-a2a-nm-00	Presented and discussed
22/07/25	IETF OPSAWG	Contribution	New version of the Internet draft on telemetry data manifest: https://www.ietf.org/archive/id/draft-ietf-opsawg-collected-	Presented and appointed for publication

			data-manifest-09.html	
22/07/25	IETF OPSAWG	Contribution	New version of the Internet draft on data provenance: https://www.ietf.org/archive/id/draft-ietf-opsawg-yang-provenance-01.html https://datatracker.ietf.org/meeting/123/materials/slides-123-opsawg-applying-cose-signatures-for-yang-data-provenance-00 https://datatracker.ietf.org/meeting/123/agenda	Presented and discussed
24/07/25	IETF RTAR Area	Presentation	Side meeting on AI agents. Presentation of the Internet draft "AI Agent protocols for 6G systems": https://www.ietf.org/archive/id/draft-stephan-ai-agent-6g-00.html https://trello.com/c/3pdVLL9w/39-1430-1630-ai-agent-protocols https://trello.com/c/v0XjZxf0/48-1100-1300-ai-agent-applications-in-6g-network	Presented
9/09/25	ETSI ZSM	Leadership	Discussions on the future of network activities within ETSI, led by the network transformation ISGs: NFV, MEC and ZSM. Presentation at ETSI Board (https://docbox.etsi.org/ISG/ZSM/05-	Discussed at the ETSO Board and the ISGs

			CONTRIBUTIONS/2025/ZSM(25)000198_ZSM_32_Meeting_Report.docx https://docbox.etsi.org/ISG/ZSM/05-CONTRIBUTIONS/2025/ZSM(25)000194_Chairman_Perspective_-_ZSM_32.pptx https://docbox.etsi.org/ISG/MEC/05-CONTRIBUTIONS/2025/MEC(25)000355_TC_DATA_Teaming_Up_in_Support_of_Open_Data_Solutions.zip https://docbox.etsi.org/Board/2025_Board/BOARD(25)Networks_004_ISG_ZSM.pptx)	
9/09/25	ETSI ZSM	Meeting	Open session with 3GPP SA5 on AI enablers and intent-driven autonomous networks follow-up https://portal.etsi.org/tb.aspx?tbid=862&SubTB=862,863#/5069-meetings	Ongoiing collaboration with 3GPP SA5
9/09/25	ETSI ZSM	Leadership	Extension request for ETSI ZSM, aligned with the convergence on network activities in the organization, presented at ETSI Boars: https://docbox.etsi.org/ISG/ZSM/05-CONTRIBUTIONS/2025/ZSM(25)000198_ZSM_32_Meeting_Report.docx https://docbox.etsi.org/Board/2025_Board/BOARD(25)154_041r1_Board_consultation_on_the_extensio	Submitted and endorsed by ETSI Board

			n_of_the_period_of_activit.docx	
10/09/25	ETSI ZSM	Leadership	Coordination with other ETSI groups on the realization of interoperability demonstration events, PLUGTESTS: https://docbox.etsi.org/ISG/ZSM/05-CONTRIBUTIONS/2025/ZSM(25)000197r1_Reply_to_ETSI_ISG_NFV_on_their_LS_on_Joint_Plugtests_Activit.docx	Coordinated with ISG NFV and other groups
10/09/25	ETSI ZSM	PoC	Update on ZSM PoC015: https://docbox.etsi.org/ISG/ZSM/05-CONTRIBUTIONS/2025/ZSM(25)000195_Update_on_PoC15.pptx https://zsmwiki.etsi.org/index.php?title=PoC_15_Trustworthy_Zero-touch_Network_and_Service_Management_in_6G_Networks_with_NDT_support	Presented and discussed at ZSM#32

Q4 2025

Date	SDO / Project / Organization	Contribution / Activity	Comments	Status Update
04/11/25	IETF Hackathon	PoC	Hackathon project demonstrating the application of schema-based provenance signatures of YANG data, via its application to Kafka schema registry: https://datatracker.ietf.org/meeting/124/materials/slides-124-hackathon-sessd-yang-provenance-signatures-integrated-with-the-kafka-schema-registry-00	Demonstrated at IETF 124
4/11/25	IETF OPSAWG	Contribution	New version and update on draft-ietf-opsawg-yang-provenance https://datatracker.ietf.org/doc/draft-ietf-opsawg-yang-provenance/ https://datatracker.ietf.org/doc/slides-124-opsawg-applying-cose-signatures-for-yang-data-provenance/	Presented and discussed at IETF 124
4/11/25	IETF WIMSE	Contribution	New version of the draft on geolocation attributes for workloads https://datatracker.ietf.org/doc/draft-lkspa-wimse-verifiable-geo-fence/	Contributed for discussion at IETF 124

4/11/25	IETF PTP	Contribution	New draft on location attestation https://datatracker.ietf.org/doc/draft-ramki-ptp-hardware-rooted-attestation/	Contributed for discussion at IETF 124
5/11/25	IETF IAB	Leadership	Intro to ETSI at IAB-Open https://datatracker.ietf.org/meeting/124/materials/slides-124-iabopen-etsi-update-01 https://datatracker.ietf.org/meeting/124/materials/minutes-124-iabopen-202511061630-00	Presented and discussed at the IAB Open meeting in IETF 124
6/11/25	IETF IVY	Contribution	New version and update on the inventory entitlement draft https://datatracker.ietf.org/doc/draft-ietf-ivy-entitlement-inventory/ https://datatracker.ietf.org/doc/slides-124-ivy-03-entitlement-inventory/	Presented and discussed at IETF 124