Horizon Europe Innovation Action

"SU-DS03-2019-2020"

Version 2
July 1st, 2021

(Submission: August 27th, 2020 - Three years / €4M)

"Digital Security and Privacy for Small and Medium Enterprises (SMEs) and Micro Enterprises (MEs)"

Towards "Instant" Deep Diffusion of Actual and Real-Time Cyber Safety Solutions through the Complete Extended Supply Networks of "Late Majority" High Value Manufacturing SMEs & MEs ("eGoose")

Maynooth University
National University of Ireland Maynooth

Proposal Coordinator: Dr. Oliver Schwabe, Principal Web Weaver, Open European Network for ENTerprise InnOVation in High Value Manufacturing (ENTOV-HVM), oliver.schwabe@innovation-web.eu.
Tel.: ++ 49 (0) 170 9053671

Website: www.innovation-web.eu Blog: https://open-european-innovation-network.blogspot.com/ Facebook: https://www.facebook.com/groups/2014779865300180/ LinkedIn Group: https://www.linkedin.com/groups/8779542/ LinkedIn Company Page: https://www.linkedin.com/company/entov Sourceforge: https://sourceforge.net/projects/entov-hvm/ Researchgate: https://www.researchgate.net/project/Open-European-Network-for-Enterprise-Innovation-in-High-Value-Manufacturing-ENTOV-HVM Twitter: @owschwabe (#innovationweb)

Challenge

"Small and Medium-sized Enterprises and Micro Enterprises (SMEs & MEs): Defenders of Security, Privacy and Personal Data Protection“ [Sub-topic (b)]

- "Most SMEs & MEs lack sufficient awareness and can only allocate limited resources - both technical and human - to counter cyber risks, hence they are an easier target (e.g. of ransomware attacks) compared to large organizations.
- Security professionals and experts working for SME s & MEs need to be in a constant learning process since cybersecurity is a significantly complex and fast-evolving field.
- Taking into account the significant economic role of SMEs & MEs in the EU, tailored research to innovation should support cybersecurity for SMEs & MEs.“

Our contribution: An innovative solution to increase the actual and real-time knowledge sharing in digital security deeply through the complete extended supply networks of SMEs, MEs and Cyber Safety Solution Providers in High Value Manufacturing.

Challenge Accepted

Principal Investigator / Dissemination & Exploitation
Prof. Markus Helfert (Professor for Digital Service Innovation, Maynooth University, Ireland)

Orchestrator / Simulation Creator
Dr. Oliver Schwabe (Principal Web Weaver at ENTOV-HVM, UK/Germany)

In-Depth Needs Analysis
Dr. Pinar Bilge (Research Group Lead at the TU Berlin, Germany)

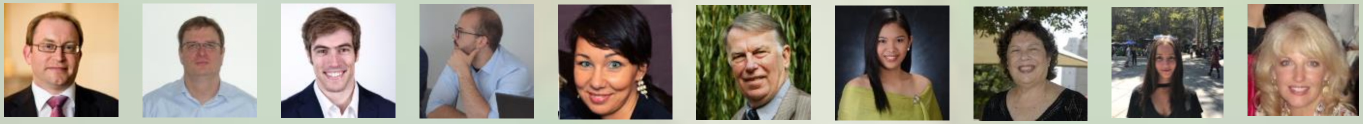
Case Studies
Prof. Nuno Almeida (University of Lisbon, Portugal)

App Creation
Dr. Ginta Majore (Vice-Rector Vidzeme University, Latvia)

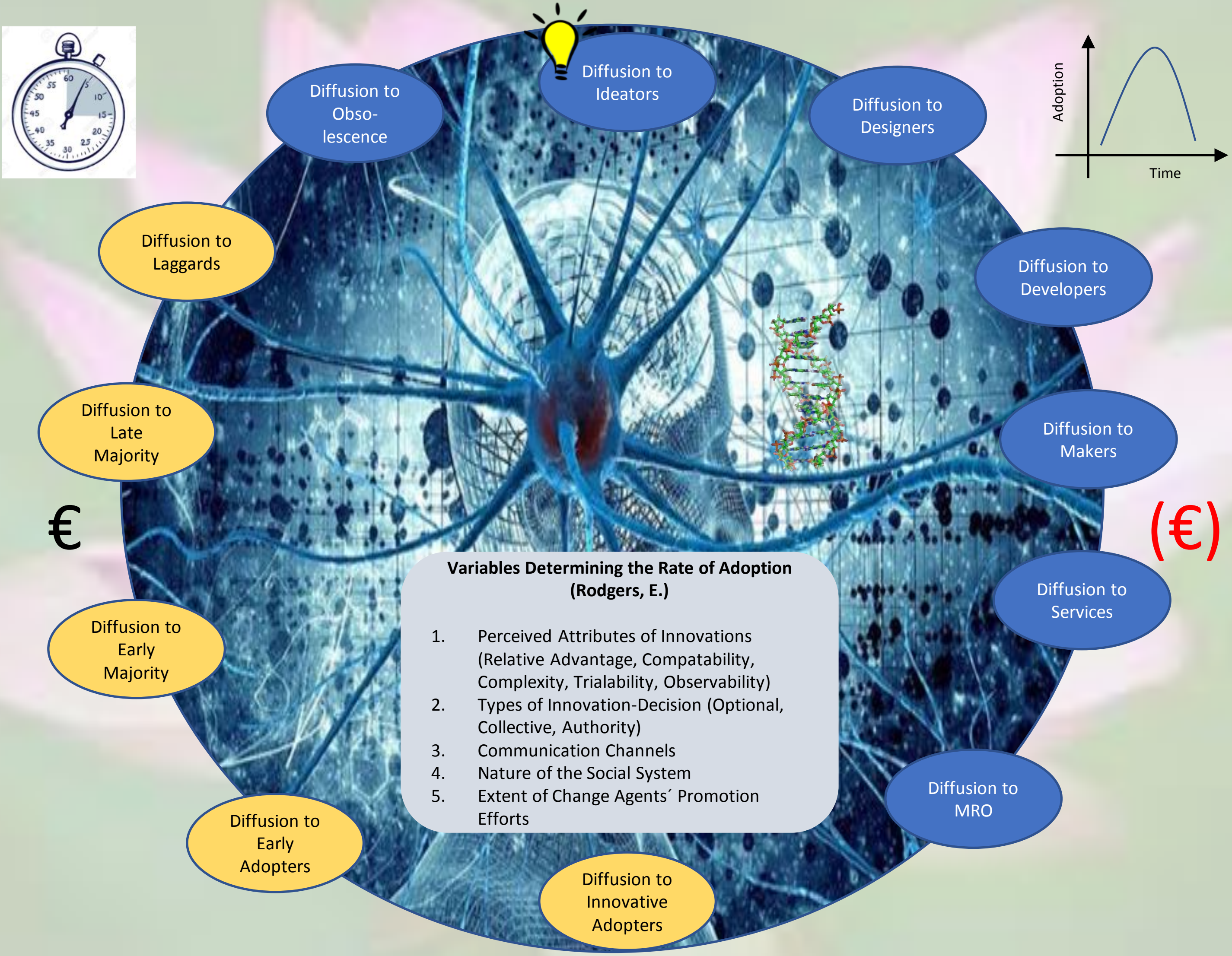
Performance Analysis
Dr. Katri Valkokari (Research Manager, VTT, Finland)

Solution Implementation
Dr. Stefano Giulitti (Research Scientist, UniSmart, Italy)

Extended Team



Response Paradigm



Diffusion to Ideators

Diffusion to Designers

Diffusion to Developers

Diffusion to Makers

Diffusion to Services

Diffusion to MRO

Diffusion to Innovative Adopters

Diffusion to Early Adopters

Diffusion to Early Majority

Diffusion to Late Majority

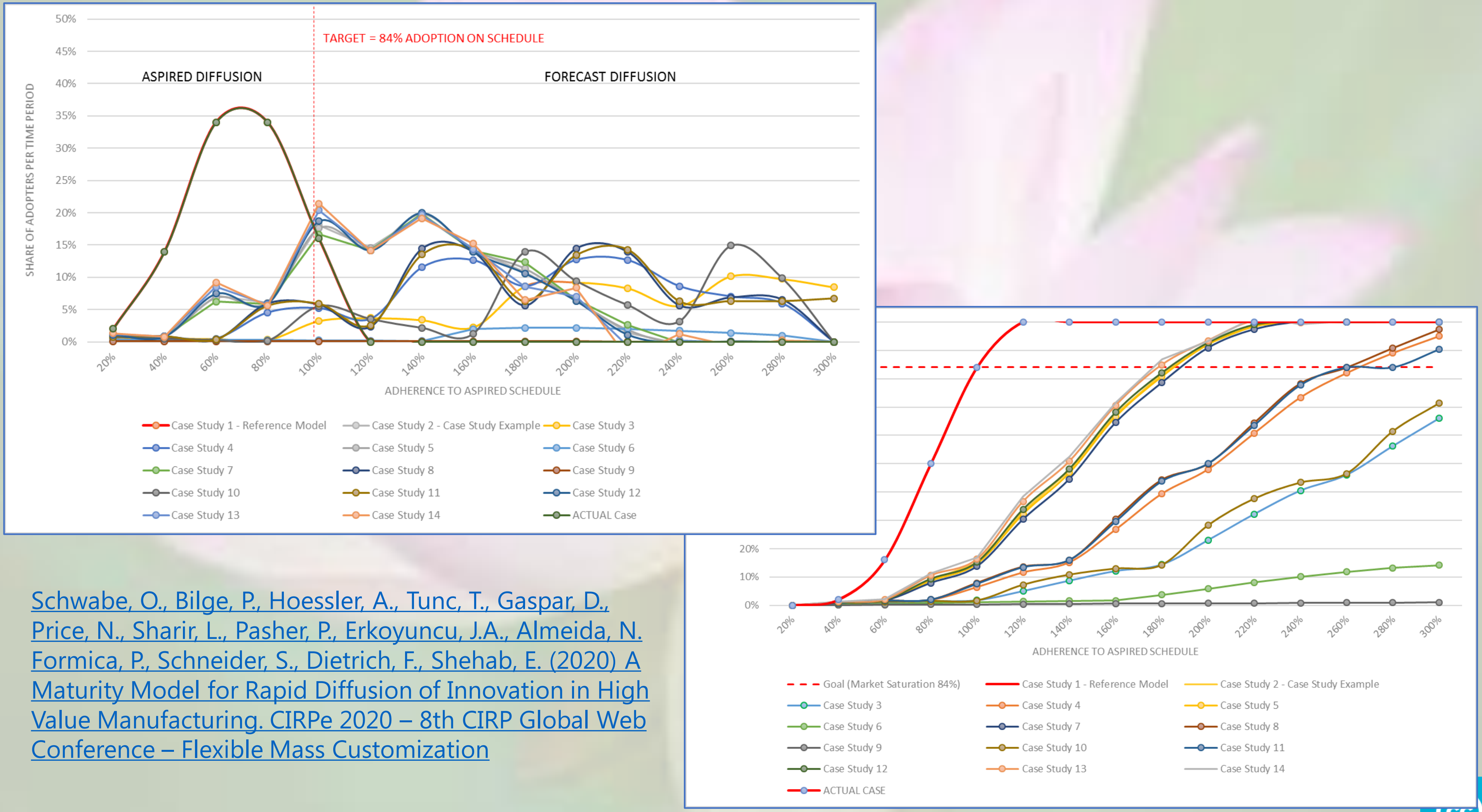
Diffusion to Laggards

Diffusion to Obso-lescence

Variables Determining the Rate of Adoption (Rodgers, E.)

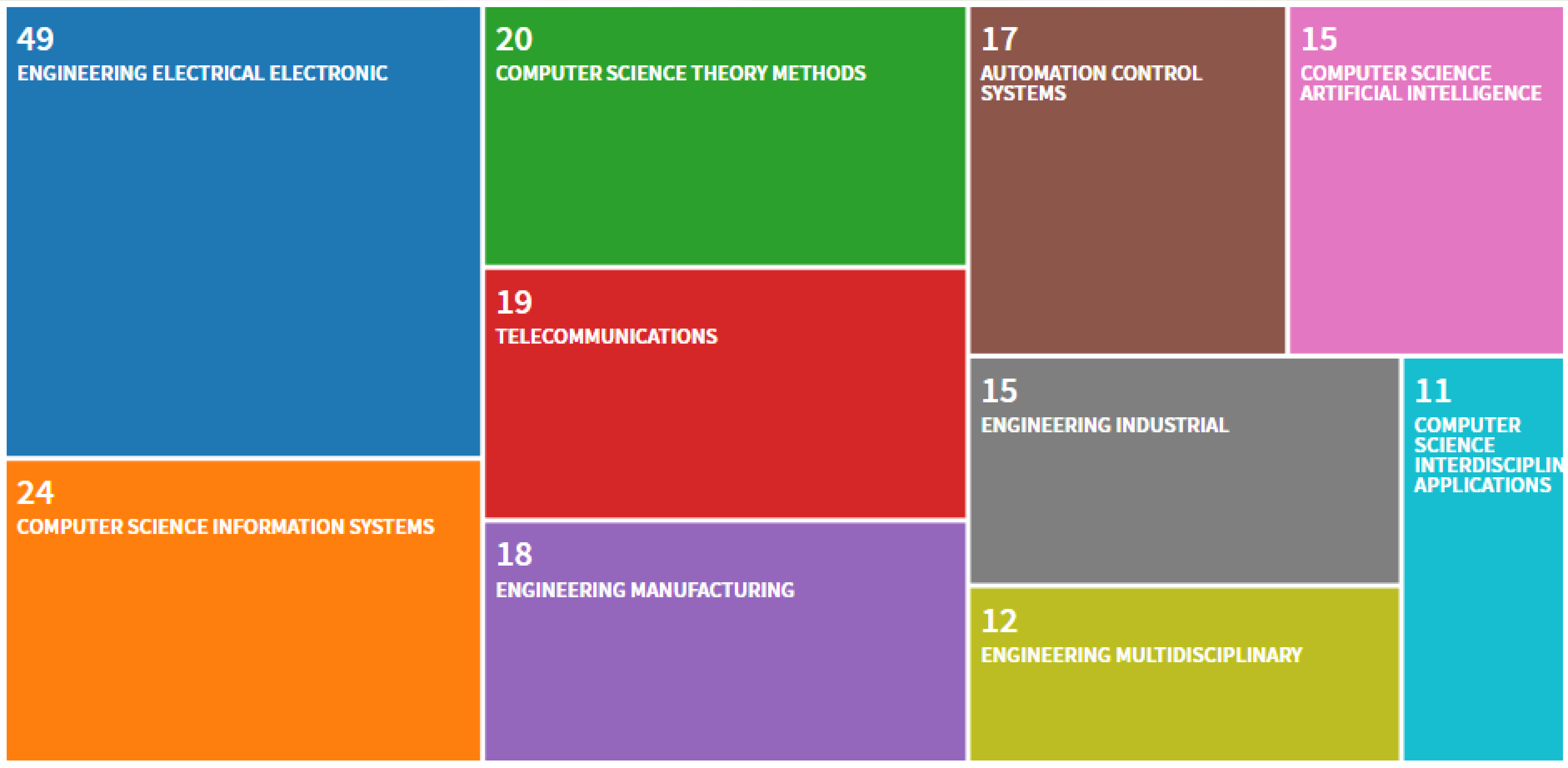
1. Perceived Attributes of Innovations (Relative Advantage, Compatability, Complexity, Trialability, Observability)
2. Types of Innovation-Decision (Optional, Collective, Authority)
3. Communication Channels
4. Nature of the Social System
5. Extent of Change Agents´ Promotion Efforts

Diffusion Challenge



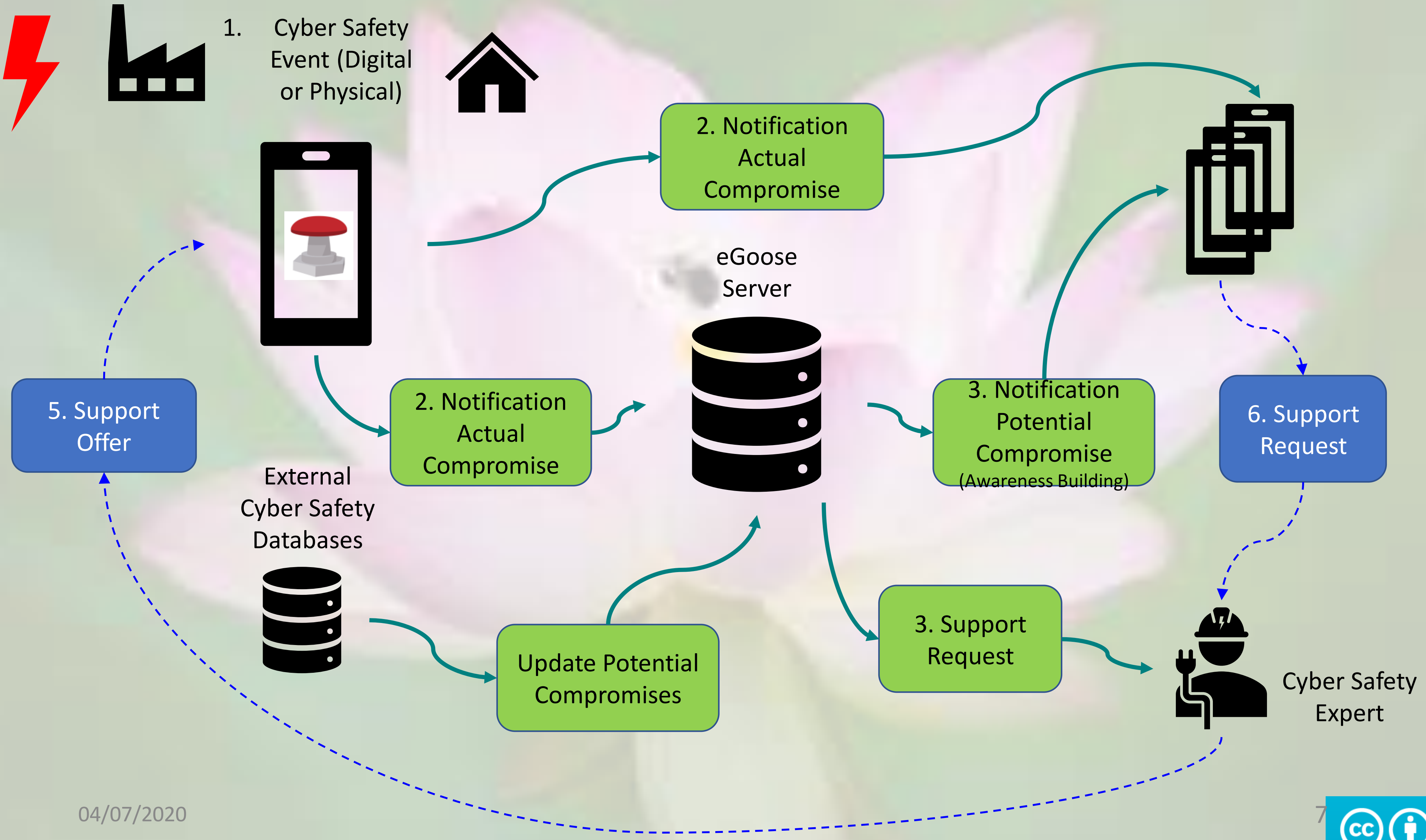
Schwabe, O., Bilge, P., Hoessler, A., Tunc, T., Gaspar, D., Price, N., Sharir, L., Pasher, P., Erkoyuncu, J.A., Almeida, N. Formica, P., Schneider, S., Dietrich, F., Shehab, E. (2020) A Maturity Model for Rapid Diffusion of Innovation in High Value Manufacturing. CIRPe 2020 – 8th CIRP Global Web Conference – Flexible Mass Customization

Scientific Pulse – "Cyber Safety In Manufacturing" – All about Technology



Data Source: Web of Science search "Cyber Safety in Manufacturing" on 20 June 2020 (153 records returned for all years in all searchable fields)

“Technical” Solution



1. Cyber Safety Event (Digital or Physical)

2. Notification Actual Compromise

2. Notification Actual Compromise

eGoose Server

3. Notification Potential Compromise (Awareness Building)

3. Support Request

5. Support Offer

6. Support Request

External Cyber Safety Databases

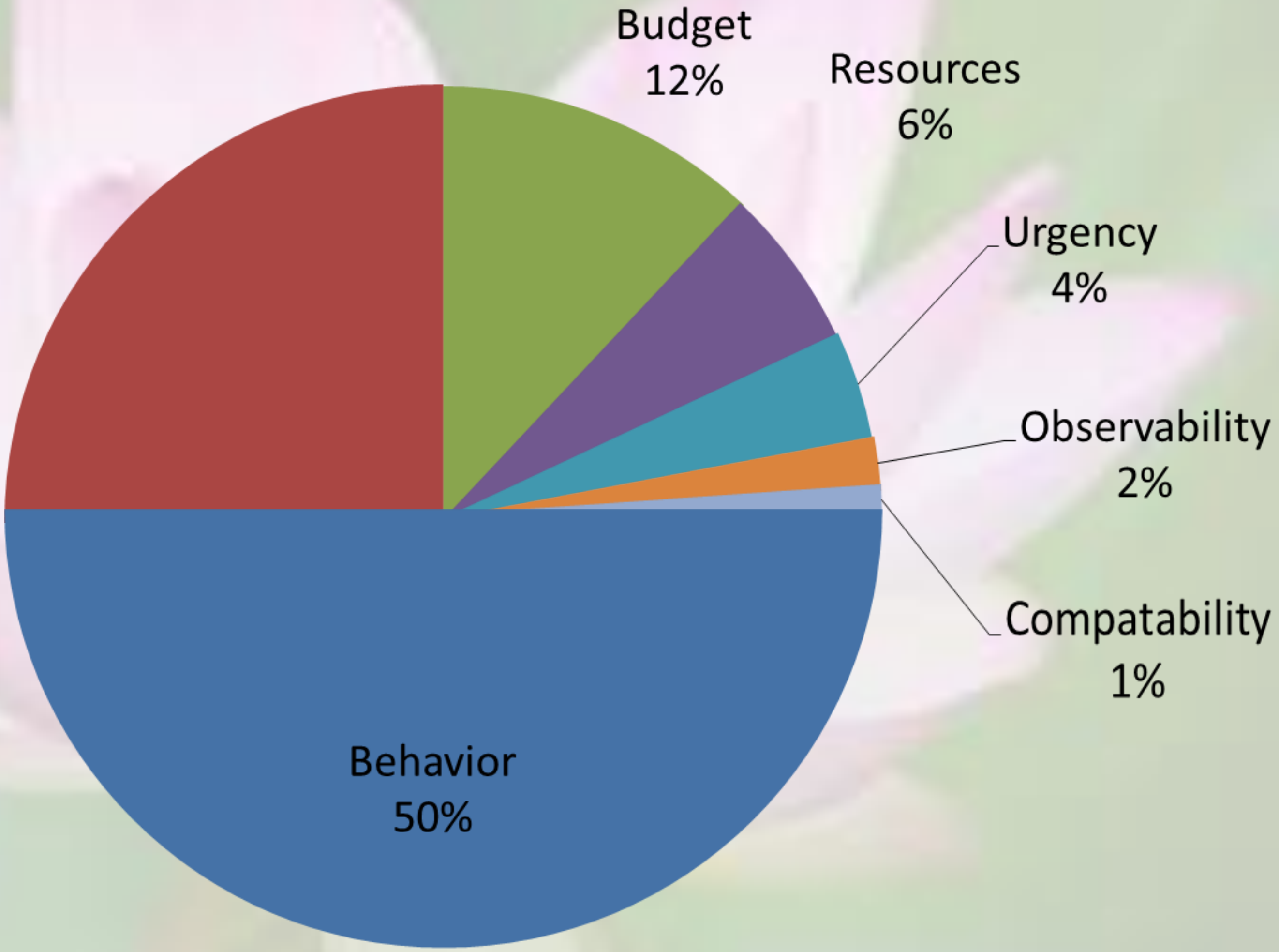
Update Potential Compromises

Cyber Safety Expert

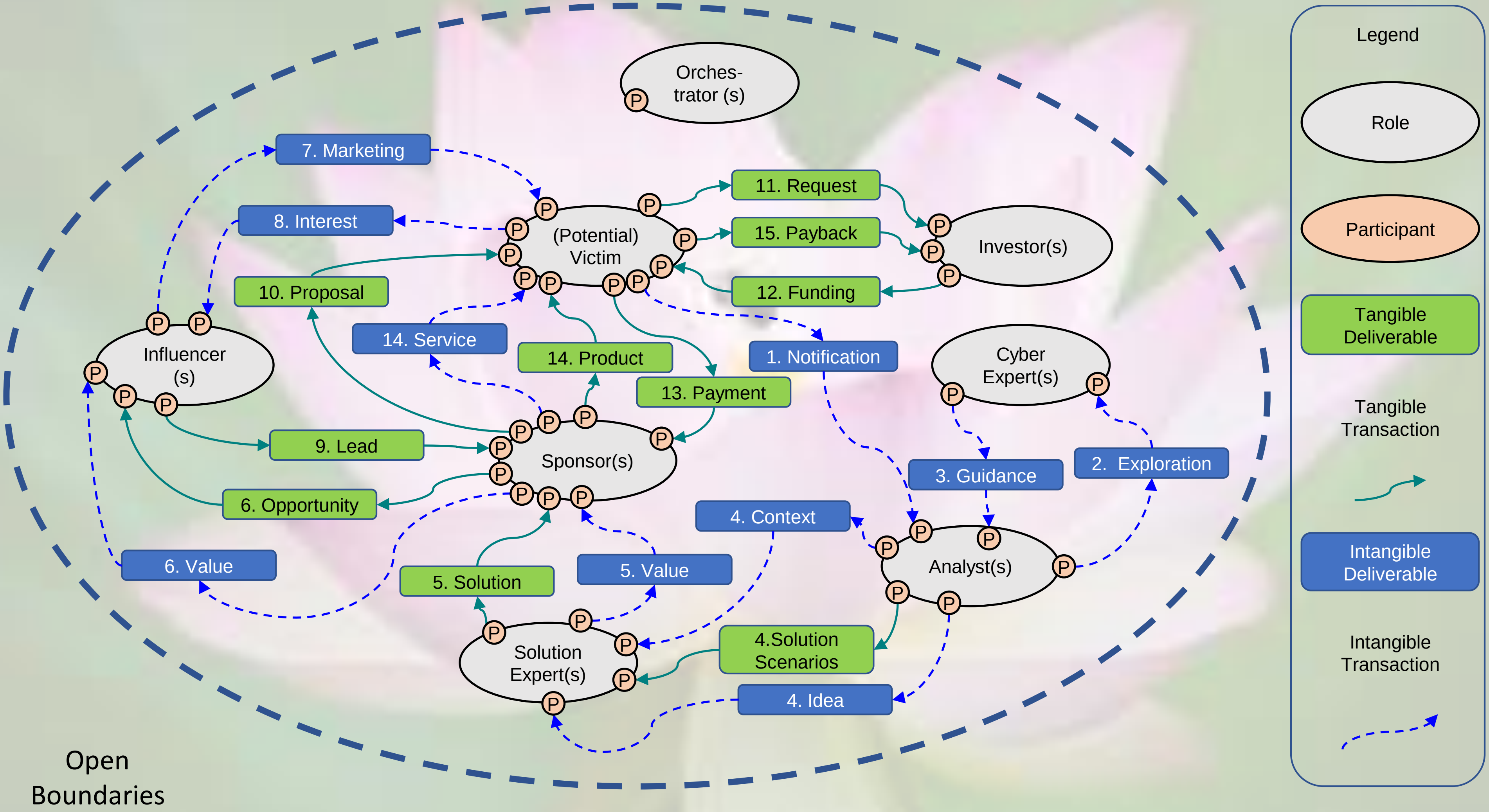
04/07/2020

Adoption Diffusion Factors

(against Planned Time to Diffusion)



“Human” Solution

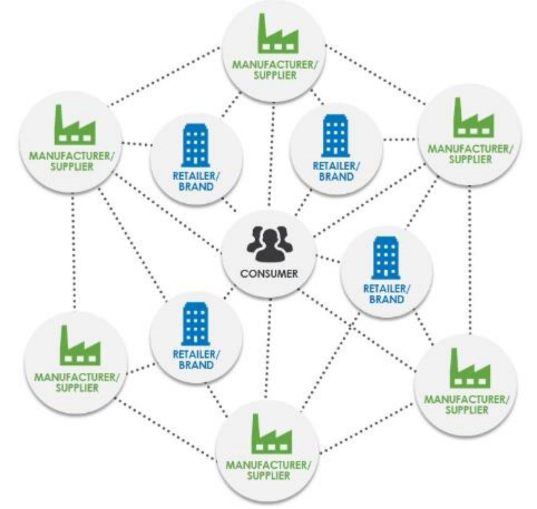


Response

The aim of our proposal is to develop and implement an innovation to help (a) continuously assess and (b) rapidly improve the Cyber Safety Effectiveness of the extended supply chain ecosystems of EU based high value manufacturing SMEs and MEs.

This aim will be achieved by an innovative solution that meets the following objectives:

1. Gather all participants of an ecosystem into a secure space.
2. Notify all participants of an ecosystem that a cyber compromise has occurred when it occurs.
3. Notify all participants of an ecosystem when a cyber compromise is expected occur.
4. Recommend suitable treatment or prevention measures.
5. Enable the creation of that “instant trust” needed among ecosystem participants to benefit from notifications and recommendations.



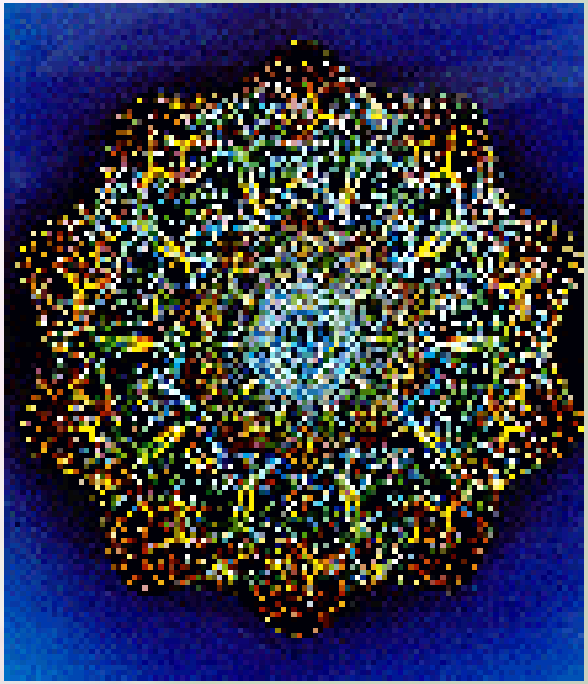
The technical element of the solution will be represented by an “app”. The social engineering required to bring the app to life within the ecosystem will be based on living systems and system dynamics models derived from research and practice.

Outcome – “Cyber Security Eco-System”

Our Action will primarily consist of activities directly aiming at producing a new process aimed at accelerating the deep diffusion of Cyber Safety solutions in high value manufacturing SME and ME supply networks. It will include prototyping, testing, demonstrating and piloting of a relevant TRL 7 solution. The pilot aims to validate the technical and economic viability of the process in an operational (or near to operational) environment. The Action will include limited research and development activities.

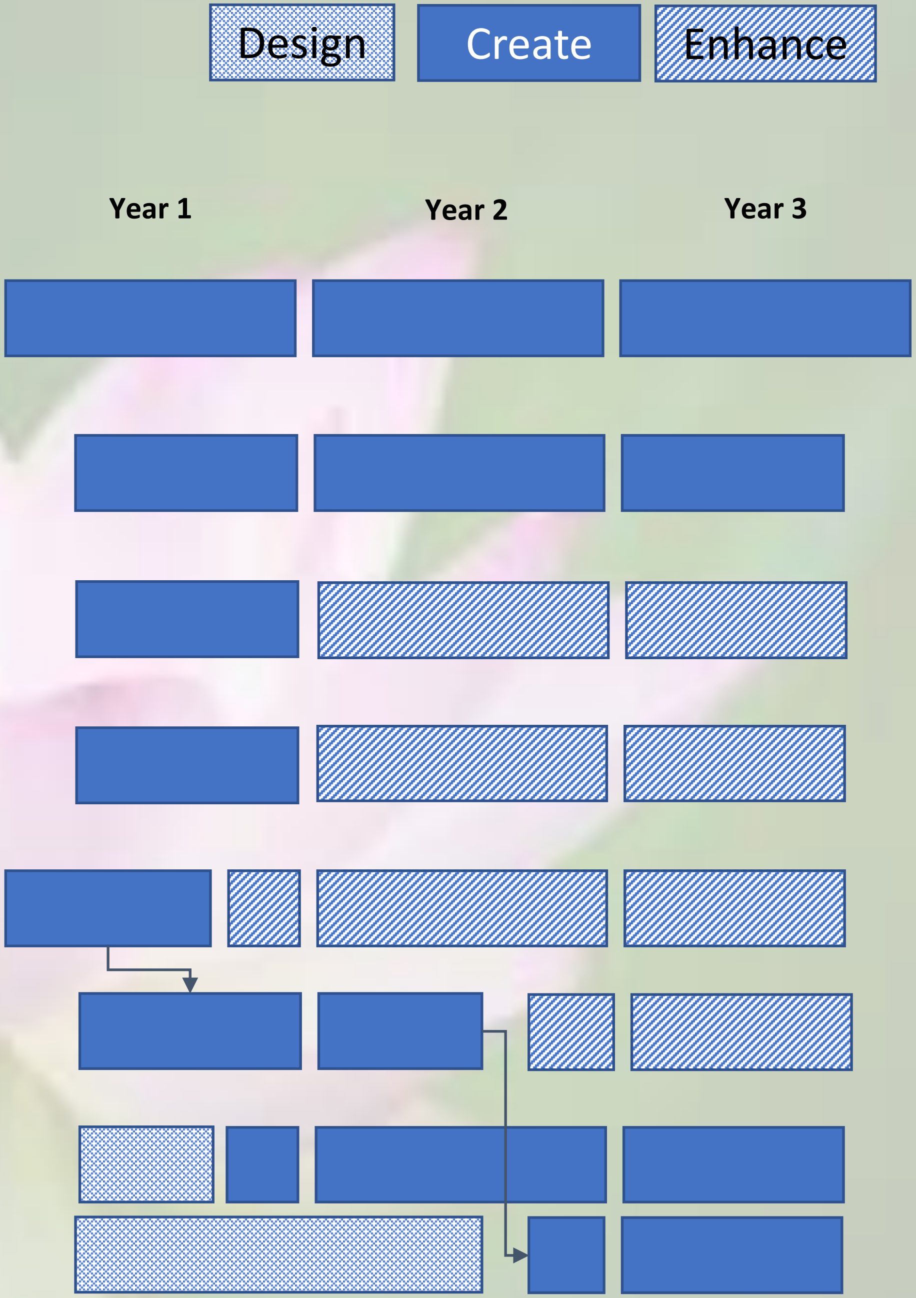
The eco-system will represent an auto-poetic / self-organizing intelligent network of deeply connected participants across their extended supply networks. The network continuously renews and recreates itself. It has cognition, perception, and complex responses.

Top Down Image of DNA



Project Plan

Work Package	Lead	Start	End	Budget %
WP 1 Management.	IE, National University of Ireland Maynooth (NUIM)	M1	M36	19%
WP 2 Dissemination and Exploitation (D&E).	IE, National University of Ireland Maynooth (NUIM)	M3	M33	9%
WP 3 In-Depth Needs Analysis.	DE, Technical University of Berlin (TUB)	M3	M12	3%
WP 4 Case Studies in Pilot Regions.	PO, University of Lisbon (LU)	M3	M12	3%
WP 5 Simulation Creation.	DE, Eurofocus International Consultants Ltd. (EF)	M1	M9	3%
WP 6 App Creation.	LV, Vidzeme University of Applied Sciences. (VUAS)	M3	M18	14%
WP 7 Performance Analysis.	FI, VTT Research Institute. (VTT)	M9	M33	11%
WP 8 Solution Implementation.	IT, UniSmart. (UNI)	M21	M33	5%



Intended Impact

The expected impact of our efforts will be that:

- SMEs & MEs are better protected and become active players in the Digital Single Market, including implementation of the NIS directive and the application of the General Data Protection Regulation.
- Security, privacy and personal data protection are strengthened as shared responsibility along all layers in the digital economy, including citizens and SMEs & MEs.
- Reduced economic damage caused by harmful cyber-attacks and privacy incidents and data (including personal data) protection breaches.
- Pave the way for a trustworthy EU digital environment benefitting all economic and social actors.
- Support and strengthen EU high value manufacturing ecosystems.

Invitation

If you have "skin in the game" for Cyber Safety and if you care about your staff / ecosystem participants and organizations you will:

- receive deep insights into how cyber safety solutions are currently deployed effectively across ecosystems by your peers and receive early access to solution as it develops,
- contribute case studies, validate research findings and host at least one workshop in their spaces each year of the project,
- pilot the developing solution in your own supply chains, and
- not required to contribute funding, nor will they receive funding.

Next Step -> Contact Us