Integrated cyber-physical security for health services

SAFECARE evaluation results

Johannes Fischbach – University of Greifswald (UG)

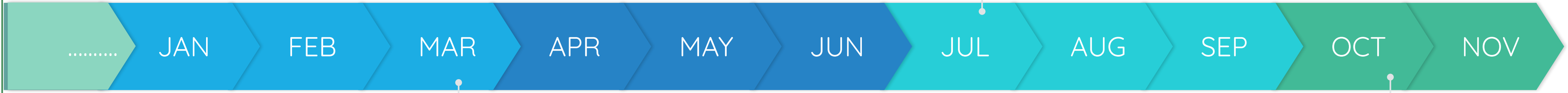
Vasiliki Mantzana – Center for Security Studies (KEMEA)

SAFECARE has received funding as part of the “Secure societies – Protecting freedom and security of Europe and its citizens” challenge of the Horizon 2020 Research and Innovation programme of the European Union under grant agreement 787002

- Introduction
- SAFECARE evaluation results (questionnaires)
- SAFECARE evaluation results (interviews)

SAFECARE demos/questionnaires timeline

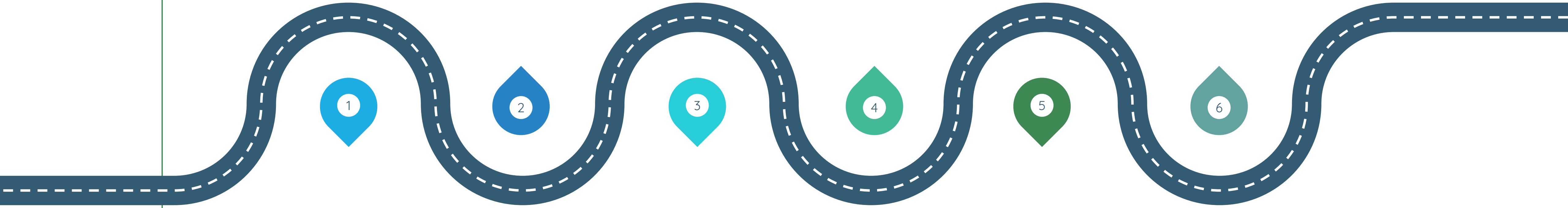
21/07/2021
Demonstration in Turin



25/03/2021
Test bed in Amsterdam

28-29/10/2021
Demonstration in Marseilles

Demonstrations’ evaluation methodology



Before demonstration:

- Scenarios to be demonstrated
- Participants (number, background, expertise etc.)
- COVID-19 restrictions

Before demonstration:

- Prepared Questionnaires and Interview agenda

Before demonstration:

- How many people will participate?
- How interviews will be contacted (physically/virtually, group/personal)?

Demonstration’s day:

- Scenarios described
- Demonstration executed
- Questions & answers
- Questionnaire filled in by end-users (Turin and Marseilles)

End of demonstration:

- Round table and general discussion
- Filling global questionnaire by end-user (Turin and Marseilles)
- Interviews (Turin and Marseilles)

After demonstration:

- Analysed data collected from questionnaires and interviews

SAFECARE scenarios demonstrated

Turin - ASLTO5

SC 2 – Cyber-physical attack to steal patient data in the hospital

SC 6 – Cyber attack on medical devices

SC 9 – Physical attack against hospital staff using a gun

SC 10 – Physical attack to steal drugs

SC 11 – Cyber-physical attack due to a personal laptop

Marseilles – AP-HM

SC 1 – Cyber-physical attack targeting power supply of the hospital

SC 3 – Cyber-physical attack targeting IT system

SC 5 – Cyber-physical attack targeting the air-cooling system of the hospital

SC 7 – Cyber-physical attack targeting the COVID-19 vaccines

SC 12 – Cyber-physical attack to block national crisis management

SAFECARE evaluation results (questionnaires)

Questionnaires

Per Scenario

- After each scenario presented the same set of items was given to the participants.
- A unique 4 character Token is generated, that enables to link all questionnaires to unique participants through the evaluation process.
- Main objective was to identify how stakeholder assess the SAFECARE system with regards to perceived quality in each scenario.

Per Demonstration

- After all scenarios have been presented a final set of items (different to scenario questionnaires) was given to the participant.
- Gather information on the overall objectives of SAFECARE from the stakeholders point of view,
- Visible module specific performance assessment by stakeholders
  - CTMS
  - HAMS
  - IPDSM
  - MAS

Questionnaires

Turin – ASLTO5

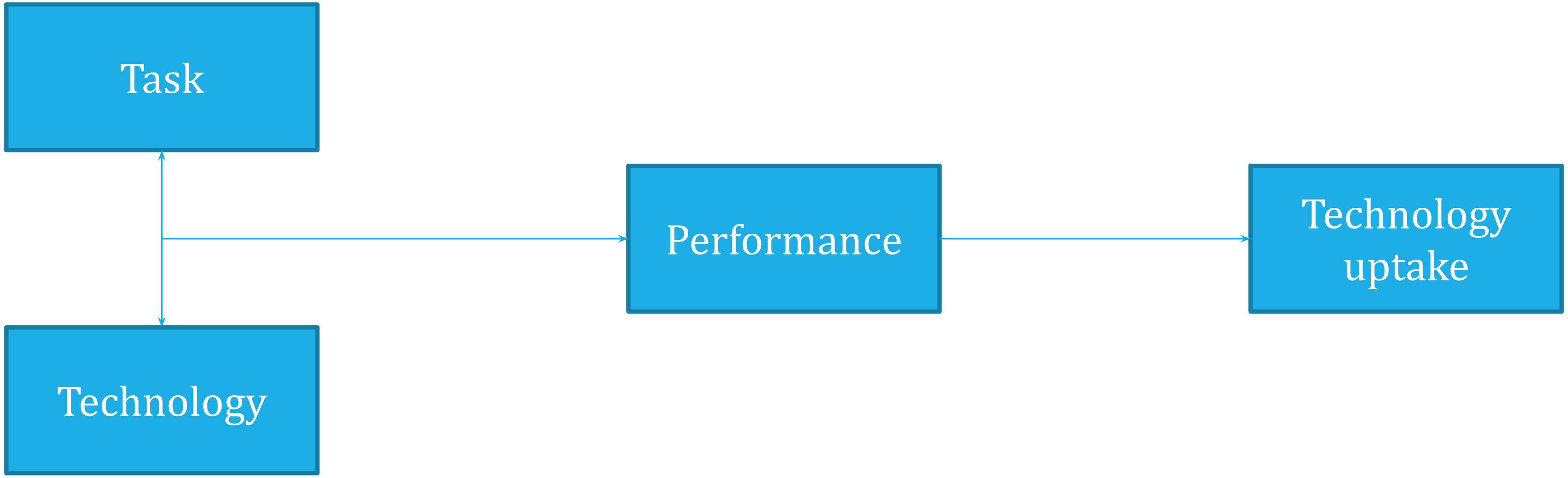
- English / Italian language
- 28 questionnaires / 6 unique participants
- Professions:
  - Health practitioners
  - Security experts
  - Firefighter
  - SOC analysts
  - Technical operators

Marseilles – AP-HM

- English / French / Italian language
- 97 questionnaires / 24 unique participants
- Professions:
  - Health practitioners
  - Security experts
  - SOC operator
  - Crisis manager
  - National and regional agencies
  - Police
  - Security officer

What makes a good System?

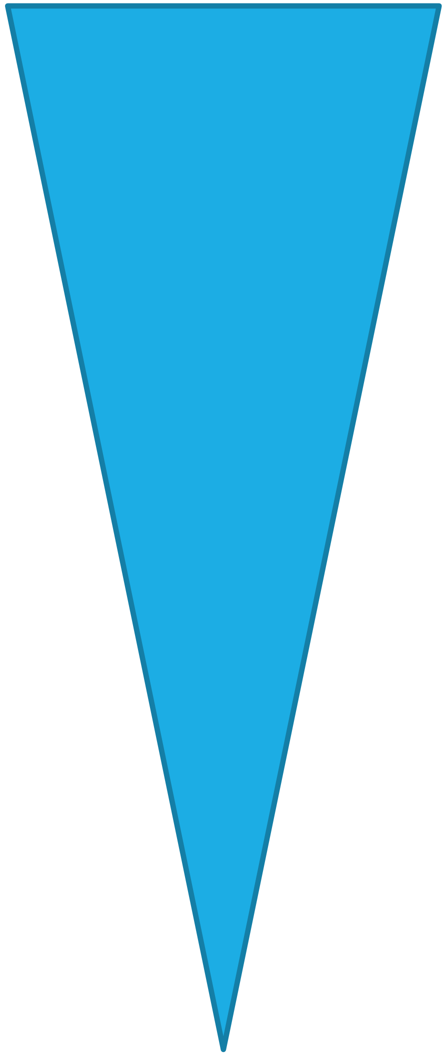
- The better the system, the better the uptake?



- Not true! → Integrate user perspective
  - Expert ratings on performance indicators
  - User attitude and technology acceptance

Way to assess a system

Expert opinions



Subjective intentions

Perceived performance of SAFECARE

Key performance indicators

Module specific performance

System Usability Score

Technology Acceptance

System performance ratings

- 81.3% of respondents completely agreed, that SAFECARE is a significant improvement over current solutions
  - Faster detection and response of cyber and physical events*

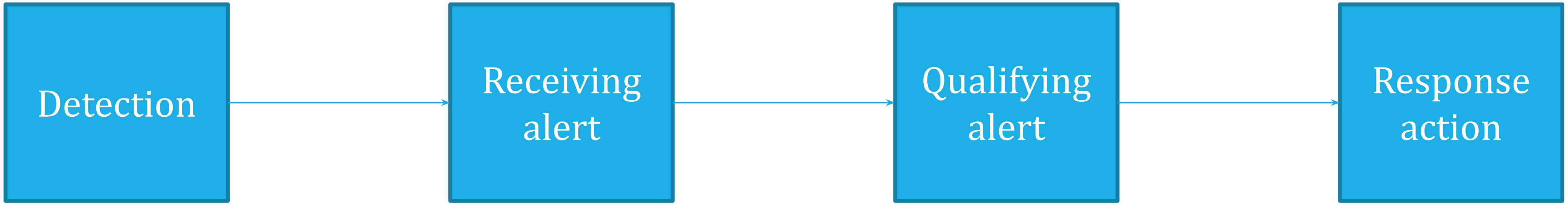
% of completely agree	cyber	physical
detection	56%	81%
response	73%	87%

*100% of respondents mostly or completely agreed

Key performance indicators

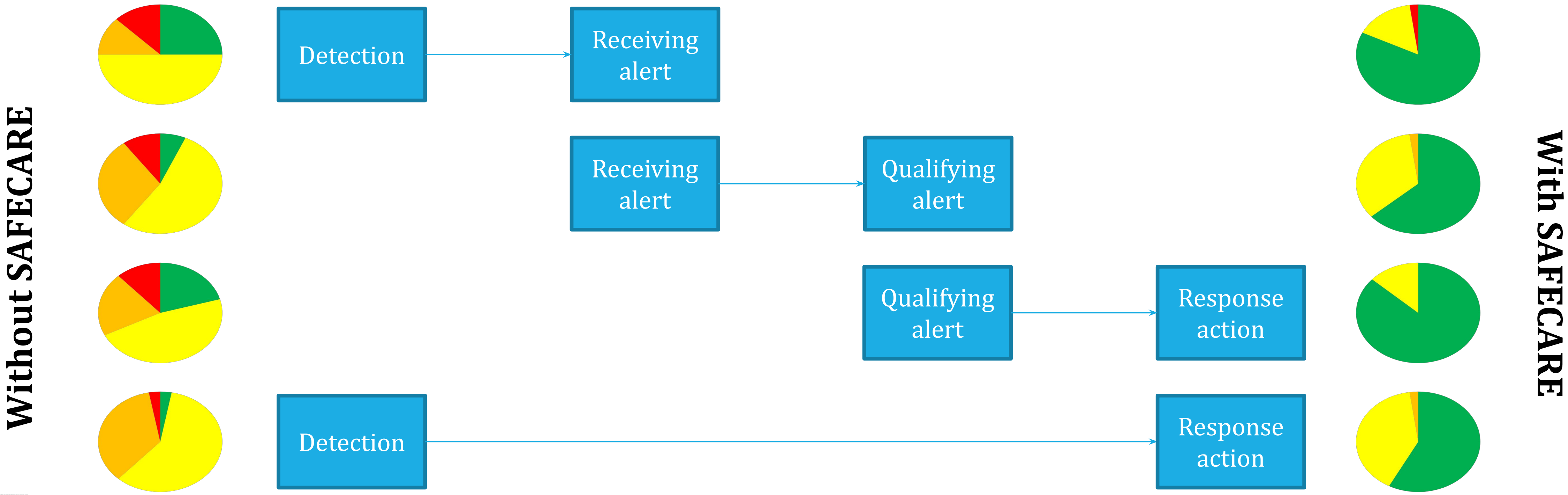
The SAFECARE system is perceived to

- Reach more agents ☺️
- Provide more modi to alert agents ☺️
- Require fewer agents to process an alert 😐
- Make better use of agents‘ skills ☺️
- Present a clearer overview over the situation ☺️
- Improve the delegation of tasks during an alert ☺️
- Decrease reaction times ☺️



Key performance indicators

- The SAFECARE system is perceived to decrease reaction times



Module specific performance

- The system modules are understood and seen as efficient and useful (1 = strongly disagree; 7 = strongly agree)

Mean values	Understood	Efficient	Useful
Cyber threat monitoring system (CTMS)	5.75	6.00	6.25
Hospital availability management system (HAMS)	5.79	6.00	6.21
Impact propagation and decision support model (IPDSM)	5.88	5.88	6.00
Mobile alerting system (MAS)	5.38	5.77	5.77
Threat response and alert system (TRAS)	6.00	6.23	6.23

System usability score

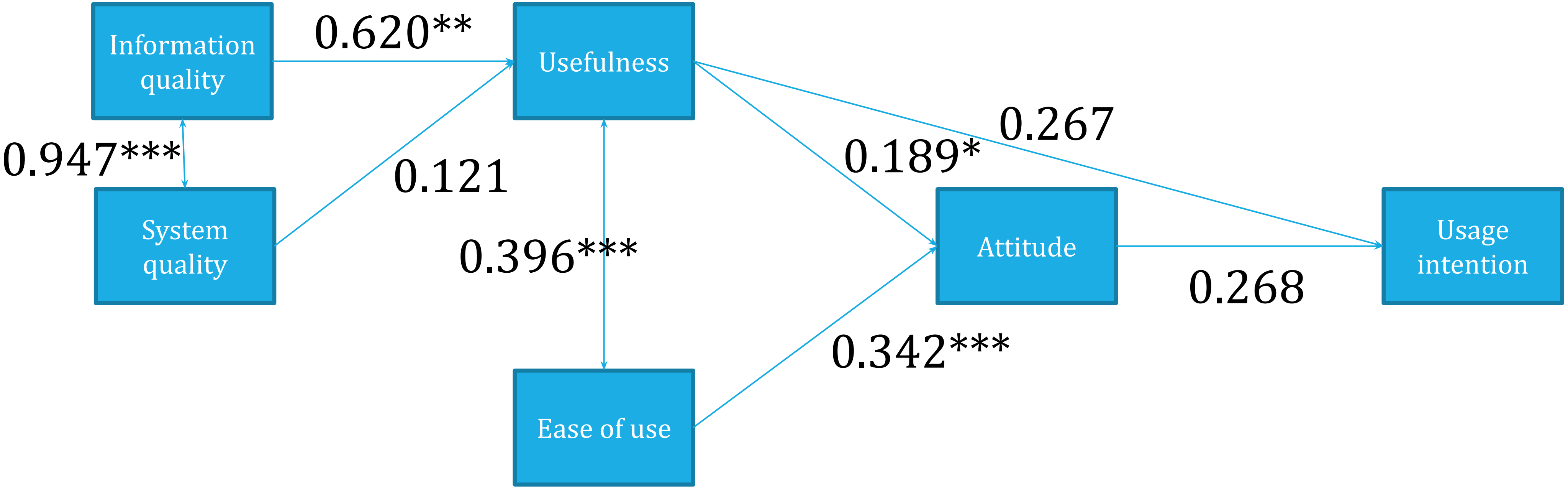
- SAFECARE scores above average on the SUS (>68)

	Turin	Marseille	Total
SUS	64.325	76.042	73.125

- It is received as a well integrated and very consistent system (4.375)
- A low mean in item 2 (1.688) suggests, that a lot of user need external support to utilise the system

Technology Acceptance

- Extended TAM:



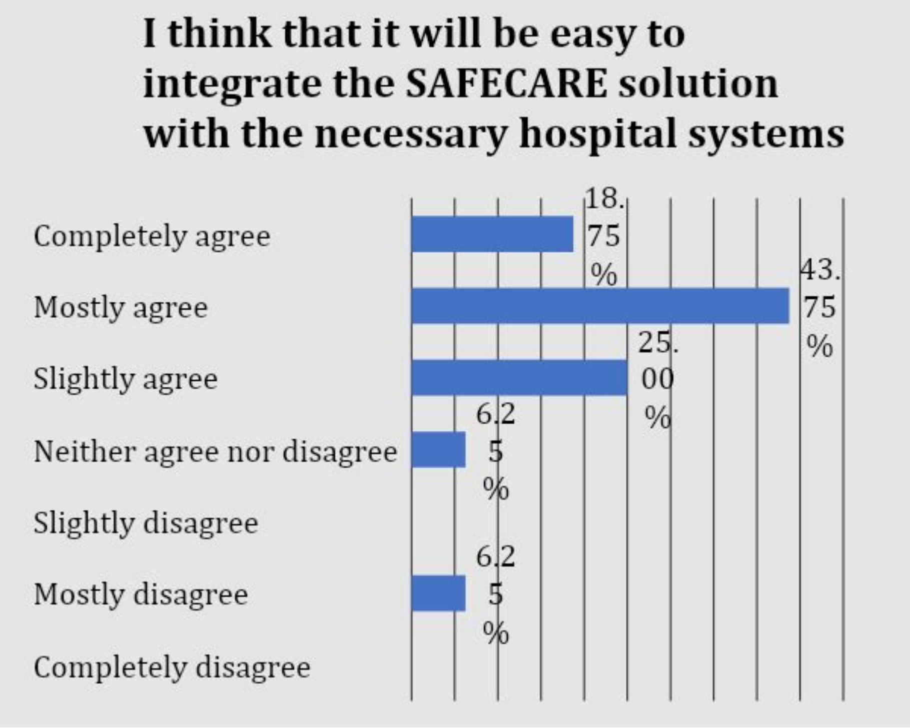
- Interaction effect of usefulness and attitude
- For pooled sample usage intention R^2=0.440

Technology Acceptance

- Completeness of information is the strongest predictor of usefulness and usage intention
- Confirms the SAFECARE approach to combine several sources of information and to provide impact propagation estimations to the user
- Out of the modules with user interaction, the threat response and alerting system (TRAS) had the highest effect on usefulness ratings (1, 51.41 F=4.438 p=0.040)

Open challanges

- Significant lower ratings from the security sector for currency, information quality, flexibility, integration, attitude and usage intention → focus more on the needs of the security sector
- Feedback
  - Open requirements
    - Study national response
    - Training / demo / simulation mode
    - More coherent view for video protection
    - Adaption to police command centre
  - Remarks
    - Include financial impacts
    - Security assessment of SAFECARE system is needed
    - Severity indices should be expressed as a percentage
  - Ethical



SAFECARE evaluation results (interviews)

SAFECARE
Integrated cyber-physical security for health services

Interview agenda – Part A

Turin - ASLTO5

- Virtually – in Italian language
- 4 interviewees
- Personnel with medical and administrative background, as well as the cyber security (SOC managers) group

Marseilles – AP-HM

- Physically – in French language
- 17 interviewees (split in 2 groups)
- Internal and external stakeholders of the hospital with medical and administrative background, IT biomedical, technical and engineering knowledge, cyber and physical security expertise, data protection management competences and security policy making responsibilities, as well as law enforcement agents

Interview agenda – Part B

Section	Aim
I. Perceived purpose of SAFECARE system	To collect data regarding perceived purpose of the SAFECARE system from the end-users' perspective and the interviewee's reason for participating.
II. End-users' expectations / requirements	To assess the extent to which SAFECARE met end-users' expectations / requirements.
III. SAFECARE system use	This set of questions is based on Critical Incident Technique and aims to identify practical problems based on usage experience with the SAFECARE system.
IV. Key success factors of SAFECARE system use	To collect data regarding the key success factors of SAFECARE system use.
V. Challenges/barriers of SAFECARE system use	To collect data regarding the challenges/barriers of SAFECARE system use.
VI. Ethical questions	To perceive the participants opinion and relevant data regarding ethical and societal issues affected by the usage of SAFECARE system.
VII. Conclusion	Conclusions / General comments.

Interview agenda – Part B

I. Perceived purpose of SAFECARE system

- aims to address, evaluate and manage **both hospital's cyber and physical threats and risks**, as well as their **impact** (through a visual map)
- provides rapidly trusted **information sharing** and supports **common operational picture**
- **enhances cooperation, communication and coordination between internal and external stakeholders** involved in crisis management process
- facilitates the **(quick and concrete) response** to security alarms
- strengthens patients, employees and assets safety and security, thus increasing the **feeling of safety to public**

Interview agenda – Part B

II. End-users' expectations / requirements

Why did they participate?

- Insights with regards to hospital's, medical equipment vulnerabilities
- Understand how cyber-physical threats could be addressed by a single system
- See how such a system can work

SAFECARE system:

- met their expectations and requirements
- characterised as very useful and pleasant to use
- can be used:
  - in hospitals, and improve its security and safety levels;
  - (If properly adapted) to other critical infrastructures and confined public spaces; and
  - at a national level, by supporting crisis management and coordination processes.

Interview agenda – Part B

III. SAFECARE system use

Scenarios

- Interesting and quite well explained
- Supported them get a comprehensive understanding of system and proved its usefulness and effectiveness
- It should be more systematically evaluated with co-designed scenarios in an operational environment (e.g. more scenarios related to different types of medical devices)

Demonstration

- Enjoyed the demo day
- Well organised demo

Interview agenda – Part B

III. SAFECARE system use

System use

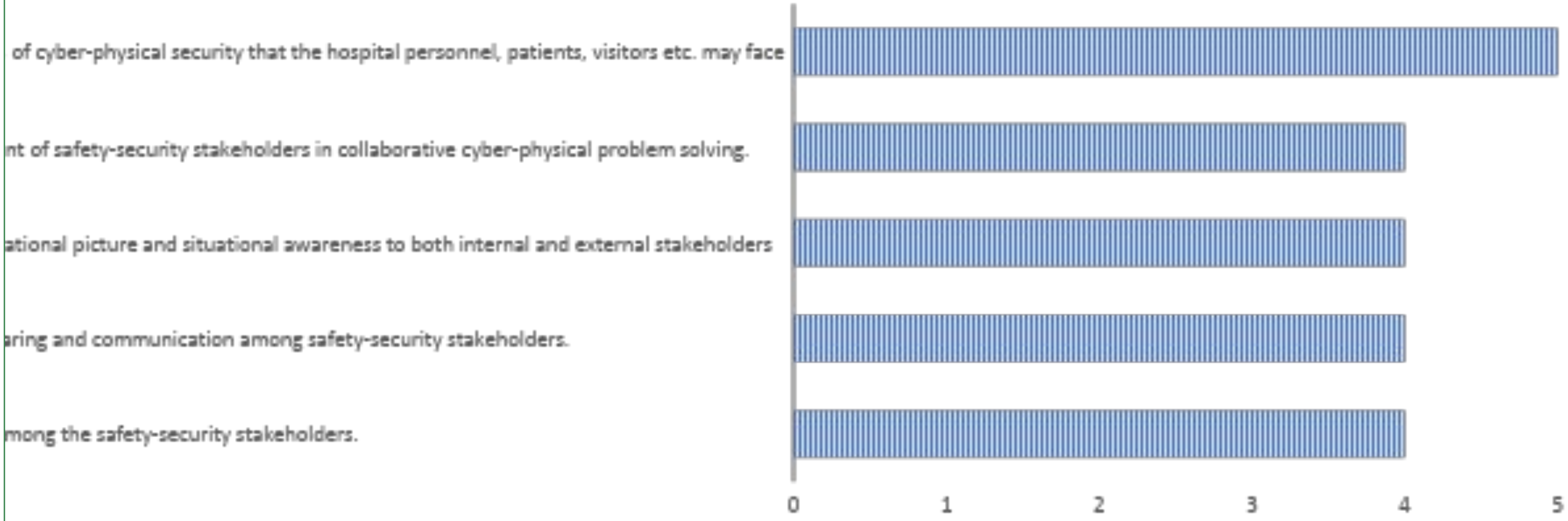
- Responds in real-time
- Provides global security supervision; combined management of cyber-physical threats
- Supports threat detection, impact analysis
- Enhances information exchange, response/mitigation cooperation and coordination between stakeholders (common operational picture)

System functionalities

- Really interesting the network scanning and the identification of attacks manifested through the hospital's network
- Impressive impact analysis and visualization functionalities

Interview agenda – Part B

IV. Key success factors of SAFECARE system use



Users' training, technical support, further evaluation and testing should be carefully considered.

Interview agenda – Part B

V. Challenges/barriers of SAFECARE system use

Challenges/barriers

- Required technical skills to run the system and keep the architecture up-to-date and maintain it.
- Personnel needs to be trained to use it.
- First responders' stated that they would prefer to receive less information (just notifications on involved actors and assets).
- Security policies should be well established, as they set the appropriate context for using such a system operationally.

Propositions for improvements

- Customization capability of system menus and components interface
- Alerts ranking provision though the notifications system
- Notification to all users when the crisis has ended
- Impact estimation (cascading effects) to other region/hospital/critical infrastructure
- System redundancy in case of internet and telephone network failure.

Interview agenda – Part B

VI. Ethical questions

- Focused on the need to explain the system and its functions very well to all the involved stakeholders
- Did not consider that the proposed system introduces any additional ethics barriers
- Existing legislation should be considered for using the system operationally
- Access rights / sharing of information should be carefully controlled

VII. General comments

- Very positive impression for the efficiency and performance of the SAFECARE system
- Impressive work has been done in the framework of this EU project
- Recommendations for further developments should be carefully taken under

SAFECARE

Integrated cyber-physical security for health services

https://www.safecare-project.eu/

@SafecareP

SAFECARE Project