Open Market Consultation Report

Results of the Open Market Consultation for the future Pre-Commercial Procurement of R&D services on the security domain to enhance the protection of public spaces against security threats related to crowd management

June 2024

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

Disclaimer and copyright

It should be noted that this document is based upon the information publicly available to the SHIELD4CROWD project and the feedback provided during the market consultation. As such, the SHIELD4CROWD project and any of its partners cannot guarantee the accuracy and/or completeness of this information and the actions and measures based upon this information. It is recommended to access the relevant EU platforms to receive the actual relevant information and updates thereof.

This document (including the accompanying annexes) has been drafted with the utmost care, but no guarantees are given regarding its soundness and/or completeness. Any errors or inaccuracies can be reported via email to: contact@shield4crowd.eu

The SHIELD4CROWD consortium is not responsible for the correct operation of any URL mentioned in this document nor for the proper functioning of any used electronic platform (for example the EU survey system). Any problems encountered when using a URL and/or an electronic platform must be reported to the organization that makes the URL or the electronic platform available. Problems with downloading and uploading (of documents) must also be reported via email to: contact@shield4crowd.eu

The SHIELD4CROWD project receives funding under the European Union's Horizon Europe framework program for research and innovation under the grant agreement No. 101121171. The EU is however not participating as a contracting authority in the procurement.

Abbreviations and acronyms

AI	Artificial Intelligence
CBRN	Chemical, biological, radiological, and nuclear
CET	Central European Time
EAFIP	European Assistance for Innovation Procurement
EC	European Commission
EU	European Union
GDPR	General Data Protection Regulation
HE	Horizon Europe
ML	Machine Learning
OMC	Open Market Consultation
PBG	Public Buyers Group
PCP	Pre-Commercial Procurement
PIN	Prior Information Notice
PTO	Public Transport Operator
R&D	Research and Development
RFI	Request For Information
SMEs	Small and Medium Enterprises
SOTA	State Of the Art
TED	Tenders Electronic Daily
TRL	Technology Readiness Level

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

Table of contents

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

1. Purpose of the Open Market Consultation

This document describes the results of the Open Market Consultation (OMC) of the project SHIELD4CROWD for the future Pre-Commercial Procurement (PCP) of Research & Development services on the security domain to enhance the protection of public spaces against security threats related to crowd management.

The OMC aimed, on the one hand, to inform technology vendors regarding the potential future PCP. On the other hand, it intended to understand their capabilities to satisfy the procurers' needs and to obtain their input on the viability of the procurement plans and conditions as described in the OMC document and annexes.

The OMC was published through a Prior Information Notice (PIN) in the Tenders Electronic Daily (TED) on 20 December 2023. The rules and objectives of the SHIELD4CROWD OMC, as well as the challenges, the potential public buyers, and the PCP approach were described in the OMC document with Annexes. This document was published on the SHIELD4CROWD website (https://shield4crowd.eu/).

Market parties were also requested to fill out a questionnaire in the EU Survey. The deadline to fill out the questionnaire was 30 May 2024. The intention of the questionnaire was to explore the market 'as-is', therefore there could not be wrong or right answers. The responses to the questionnaire could not contain any confidential information. The information obtained will be used as input for the procurement strategy and conditions.

The OMC was performed under the law of the Lead Procurer - Société Nationale des chemins de fer (SNCF) - which is French law.

After processing the questions and responses of all suppliers, this document has the objective of communicating the results to the market. In this context, all information provided by technology vendors is treated as commercially sensitive and specific details will not be communicated to any supplier. Only the general findings are summarised and communicated in this report. This anonymised report (excluding confidential information) will be published in June 2024 on the SHIELD4CROWD website (https://shield4crowd.eu/).

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

By carrying out the open market consultation, the procurers do not commit to subsequently deploying a procurement procedure. Moreover, in case this OMC will be followed by a procurement procedure, the public procurers reserve the right to change any elements that define the desired solution. No rights can be derived from any statements made by the procurers during the OMC. Participation in the OMC is not a precondition for bidding in the future PCP.

The data collected, processed, stored, and used by the SHIELD4CROWD Consortium has the only purpose of implementing the SHIELD4CROWD project and is handled according to the General Data Protection Regulation (Regulation 2016/679 of the European Parliament and the Council - GDPR). Participants may exercise their right to access their personal data and the right to rectify such data by contacting: contact@shield4crowd.eu

2. Activities & timetable

The OMC took place in the form of:

- A series of online OMC webinars in 5 different EU languages (English, French, Slovak, Italian and Spanish).
- An OMC Event in Warsaw (Poland) on 14 May 2024.
- A Request for Information (RFI) – a questionnaire using the EU Survey tool.

The timetable for the OMC was set as follows:

Date	Event
20 December 2023	Publication of the Prior Information Notice (PIN) on TED.
22 March 2024	Publication of the OMC documents on the project's website: www.shield4crowd.eu Publication of the EU Survey questionnaire: https://ec.europa.eu/eusurvey/runner/shield4crowd

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

2 April 2024	OMC Event in English (online) (10:00 – 11:30 CET)
3 April 2024	OMC Event in French (online) (10:00 – 11:30 CET)
4 April 2024	OMC Event in Italian (online) (10:00 – 11:30 CET)
4 April 2024	OMC Event in Slovakian (online) (12:00 – 13:30 CET)
5 April 2024	OMC Event in Spanish (online) (10:00 – 11:30 CET)
14 May 2024	OMC Event in Warsaw, Poland (hybrid) (9:00 – 13:00 CET)
30 May 2024	Deadline for filling in the OMC questionnaire (17:00 CET)
10 June 2024	Publication of the OMC report.
11 June 2024	Closure of the OMC.

Table 1.- OMC timetable.

Parties interested in participating in the five (5) online events were requested to register through an online form. A total of 106 people registered for the OMC webinars, including people from public organizations, private organizations, start-ups, SMEs, and others. A total of forty (40) attendees participated in the English event, thirty-six (36) in the French, thirty (30) in the Slovakian, twenty-one (21) in the Spanish, and finally eight (8) in the Italian one. The agendas of the OMC webinars are included in Annex I.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

The main event in Warsaw was followed by eighty-two (82) attendees. A total of forty-two (42) people attended the event onsite, while the other forty (40) participated online. The agenda of this event is attached as Annex II.

The webinars within the framework of the OMC and the hybrid event in Warsaw were recorded. The video recordings are available on the SHIELD4CROWD website (https://shield4crowd.eu/).

Along with the events and RfI questionnaire, the SHIELD4CROWD Consortium organised a matchmaking event to facilitate synergies among technology providers, and several e-pitching sessions to understand the solutions available on the market, as described below.

2.1. Matchmaking event

In the context of the Open Market Consultation of SHIELD4CROWD, a matchmaking session was organised to allow the technology providers to present their companies and explore potential synergies for a potential consortium in a future PCP. Thirty-two (32) companies participated online and six (6) onsite.

Following the presentations of participants in the venue and online, the matchmaking session took place in the form of a speed date where all the participants had the opportunity to talk to each other. After the speed date, a group discussion was organised to address questions. Finally, a plenary session was held to gather insights from the participants, including the public buyers.

The main topics addressed during the group discussion were:

- The PCP phases, its competitive approach where several providers can participate in consortia, and the budget allocation in the PCP. Some participants were not aware of the characteristics of the PCP procedure.
- The timeline for the future PCP was of interest to all the participants. It was explained that the process will depend on the times of the HE PCP call and the

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

award of the grant to start the PCP tender which may be launched at the start of 2026.

- The participants expressed some concerns about the waiting time between phases.
- The IPR vested in the contractors, their management and exploitation were relevant topics for the participants.
- The possibility of presenting bids in consortia was also discussed. The participants were interested in joining efforts with bigger companies and research institutions.
- It was suggested that the R&D activities should not be linear but iterative as in an agile approach, providing room for adjustments if needed.
- The participants highlighted the importance of setting up a good methodology to prepare and assess the pilots.

Additionally, a matchmaking form is available on the project's website for those technology providers who want to get in touch with other companies.

2.2. E-pitching sessions

Along with the OMC activities, a series of e-pitching sessions were organised to complement the results of the market analysis and better understand the solutions available in the market as well as the R&D capabilities of the technology providers to address the three scenarios proposed by SHIELD4CROWD.

The e-pitching sessions were conducted on the 15th, 16th and 17th of April 2024. Each day of e-pitching sessions was dedicated to one of the three scenarios of the project. A total of fifty (50) technology providers pitched their solutions and ongoing research to the public buyers and members of the SHIELD4CROWD Consortium.

The anonymised results of the e-pitching sessions are detailed in Annex III.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

3. The Open Market Consultation results

3.1 Procedure and reporting

The OMC started on the date of its publication in the EU's Supplement to the Official Journal (TED) and ended on the date set in the timetable above.

Interested parties were requested to register in order to participate in the events and receive additional information about the project. Additional written contribution in the form of a Request for Information (RFI) questionnaire was requested through the EU Survey questionnaire. The responses to the questionnaire could not contain any confidential information. The questionnaire was intended to explore the market 'as is', there are no wrong or right answers. The answers provided will be used as input for the procurement strategy and contract conditions.

The SHIELD4CROWD Consortium supported interested parties throughout the whole OMC during the webinars, the hybrid event in Warsaw, and by answering questions through a Q&A document that was published on the project's website.

Market operators who wished to provide additional confidential information during the OMC could send this to the email: contact@shield4crowd.eu. The information had to be clearly marked as confidential. Confidential information is not included in the OMC report.

The language of this OMC is English.

3.2 Open Market Consultation report

After processing and analyzing the feedback from the market, the SHIELD4CROWD Consortium aims to disseminate the results to the widest possible audience through this

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

OMC report. Nevertheless, all answers provided by the technology providers are anonymized. The SHIELD4CROWD Consortium will, therefore, provide only the general findings and a summary of the answers obtained in the EU Survey questionnaire. The OMC Report is published on the website of SHIELD4CROWD.

Based on the feedback provided in the EU Survey questionnaire, the majority of respondents belong to start-ups and SMEs, as indicated in the figure below.

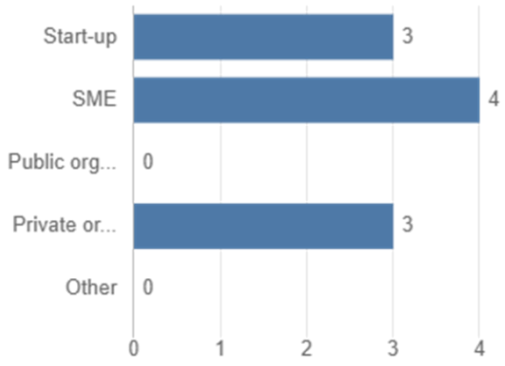


Figure 1.- Type of organizations who replied to the Request for Information using the EU Survey tool.

A total of ten (10) technology providers replied to the EU Survey questionnaire. They were from organizations located in France, Sweden, and Poland.

3.3 Summary of the replies to the EU Survey questionnaire (Request for Information)

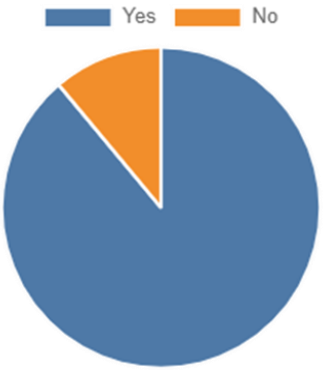
This section summarises the feedback provided to each of the twenty-two questions of the EU Survey under three topics: (1) The PCP challenge and requirements; (2) The State-Of-The-Art analysis; and (3) Miscellaneous.

3.3.1 The PCP challenge and requirements

1. Do you know any technological developments to protect public spaces in EU cities against security threats related to crowd management that SHIELD4CROWD needs to take into account?

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

Most respondents answered positively to this question (see Figure 2).



Yes	8
No	1
No answer	1

Figure 2.- Answers regarding technological developments addressing security threats related to crowd management.

A summary of the answers is provided below:

- One respondent emphasized that utilizing a blend of video, audio, sensors, AI analytics, and monitoring tools enables proactive responses to security threats. Predictive analysis aids in anticipating incidents, such as detecting anomalies like increased crowd sizes. Protection involves vigilant monitoring and analysis of crowd behaviour, ensuring timely intervention with available resources.
- Another respondent has identified three main pillars on which the solution to be developed in the future PCP should be based: crisis management, video analytics and capturing real-time information related to a relevant event. Crisis Management must be positioned as an integration platform to bring together all components of the solution. Additionally, it should lead to the identification and pushing of relevant information to stakeholders by collecting data based on standard operating procedures and exchange rules to oversee decisions & manage actions related to the crisis. Finally, it should support multi-channel communication capabilities (voice and non-voice) and map-based information presentation to secure an unhindered communication network.

  As for the video analytics, it should be the main source of information as it can be based on the existing cameras network, providing a vast geo-coverage at low cost (no installation needed), to detect many anomalous situations before the event (such as crowd panic, crowd grouping, violence and aggression,

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

loitering, or abandoned objects) and to collect real-time information during the event (counting people in an area, detecting bottlenecks for evacuation, detecting traffic jams for access to the site, etc.), while selecting the video streams to be sent to end-users on the field (police, emergency services, fire brigade) enriched with analysis data (alarm, count, direction, facial recognition data if allowed, etc.).

- Other respondents revealed more technological developments to protect public spaces in EU cities against security threats related to crowd management. Some suggestions include audio surveillance, increased hardware capacity to implement real-time video analysis, anti-terrorism free-standing barriers, a decision support framework with gaming and simulation elements, anti-drone devices, and electro-optical and stereoscopic detection tools.
- Ultimately, a technology provider discussed standalone radiological detectors which some want to develop and integrate chemical detection for CWA (Chemical Warfare Agents) and TIC (Toxic Industrial Chemicals) threats. Sensor technology will be based on FAIMS (Field asymmetric Ion mobility spectrometry).

2. Do you foresee any barriers to implement the potential solution?

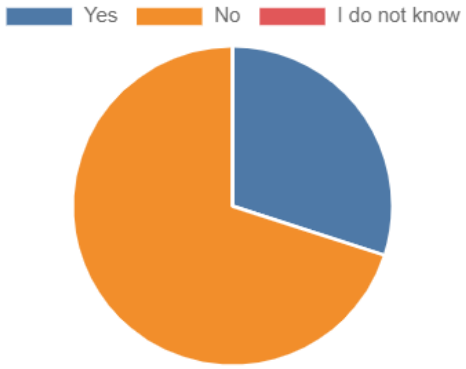
The majority of respondents do not foresee any barriers to the implementation of the potential solution. Nevertheless, some participants identified certain aspects that should be considered.

One respondent foresees potential barriers on the technical side of things. Finding a holistic solution that combines every sensor, software and hardware into one usable system will be a challenge. The system format and specifications may cause some issues concerning its deployment, functionality and effectiveness. Additionally, identifying the right people to use and receive the right parts of information and defining who will have access to the system appears to be a challenge. Finally, the

concepts of honesty and bias that each entity brings to the table may influence the final solution, its structure, and its functionalities.

Another potential barrier would be getting authorizations to develop and assess a system in real-life situations (due to personal and sensitive data) as well as difficulties in identifying a test site where the envisioned scenarios sometimes really happen (unusual crowd movements).

Lastly, a participant pinpointed that miniaturizing a gas sensor capable of detecting and discriminating various kinds of threats would be technically challenging.



Yes	3
No	7
I don't know	0

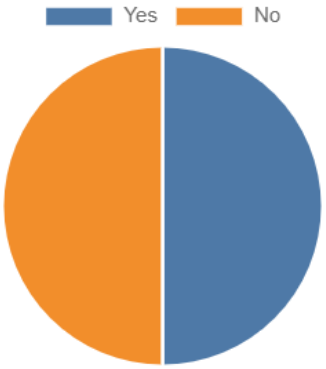
Figure 3.- Answers regarding potential barriers.

3. Can you identify relevant needs that have not been described in the market consultation document?

As illustrated in Figure 4 below, half of the respondents could identify relevant needs that were not described in the market consultation document, while the other half could not.

Yes	5

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171



No	5

Figure 4.- Answers regarding the relevant needs.

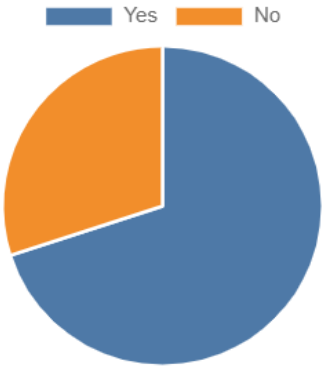
A summary of the answers provided can be found below:

- A participant asked for more information on the final use case to identify potential gaps.
- Other respondents believe they would need more details concerning data protection and privacy requirements (i.e. GDPR – General Data Protection Regulation) to set the proper framework.
- Voice and video conferencing needs are not specified.
- The case of multimedia file sharing between stakeholders during crisis situations needs to be considered.
- Some doubts have been raised concerning the status of infrastructure and sensors, issues with their installation as well as critical telecommunications handling.
- Finally, other economic operators propose solutions for crisis management encompassing the development of an ergonomic interface for efficient analysis setup and facilitating the creation of statistical and quantitative anonymized data derived from video analysis. This interface enhances the interaction between surveillance devices and the control centre, streamlining processes for data capture, protocol adherence, and legal limitations such as those imposed by GDPR regulations, including considerations for audio recording permissions.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

4. Do you have knowledge of any suitable technology or combination of technologies that can address the use case "Coordinated bomb and CBRN attacks during major sport events"? & Can this technology or combination of technologies tackle one or more of the prioritised steps in order of importance: (1) Detect/Alert, (2) Assess/Follow, and (3) Resolve? Please elaborate.

The majority of respondents answered that their solutions and technologies are suitable to address the challenge in question (see Figure 5).



Yes	7
No	3

Figure 5.- Answers regarding technologies that can address scenario 1.

A summary of the answers received can be found below:

- A technology provider proposed a system for managing security situations involving pre-, during, and post-event monitoring and response. Pre-event includes monitoring authorized entries, standard surveillance, and employing diverse technologies to prevent unauthorized items from entering. During the event, monitoring identifies disturbances and analyses factors like behaviour and environmental threats. Post-event focuses on resource allocation, traffic management, and guiding first responders. Education on sensor capabilities is crucial, especially for a diverse user base, covering visuals, thermal, radar, audio, and environmental sensors to address blind spots like fire.
- Another participant suggested a comprehensive solution for managing coordinated bomb and CBRN attacks during major events, comprising Crisis Management as the core component and Video Analytics for detection/alert

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

and assessment/follow-up. Video Analytics detects abnormal situations and provides real-time information for public safety, threat identification, and stakeholder support. Additional components may include drone activity detectors, CRBN sensors, and drone data collection to enhance detection and assessment capabilities. It anticipates minimal improvement needs for the proposed sensors/solutions, focusing primarily on integration.

- The utilization of video analytics and the use of a crisis management platform were also proposed by the respondents.
- A different proposal focuses on Application Programming Interfaces (APIs) connectivity in order to qualify threats through hypervision technology combining it with different threat detection technologies.
- Drone detection technology along with audio surveillance tools and protocols complete the frame of proposed solutions regarding this challenge.

Concerning the prioritised steps, some respondents claimed that their technological solutions could tackle one or several of them.

5. Do you have knowledge of any suitable technology or combination of technologies that cover the use case "Concert venue chaos: disinformation – induced panic"? Can this technology or combination of technologies tackle one or more of the prioritised steps in order of importance: (1) Assess/Follow, (2) Prevent/Protect, (3) Resolve, and (4) Detect/Alert? Please elaborate.

The majority of respondents answered positively to this question, claiming that their solutions and technologies are suitable to address the challenge in question.

Yes	6
No	4

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

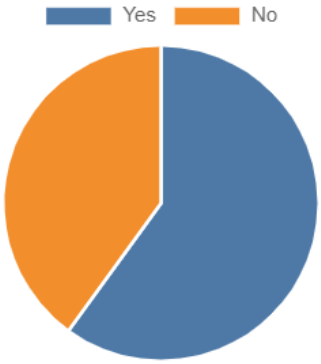


Figure 6.- Answers regarding technologies that can address scenario 2.

A summary of the answers received can be found below:

- A technology provider proposed a system for event security management involving three phases: pre-, during, and post-event, all integrated into one comprehensive system. Pre-event activities include monitoring authorized access, employing diverse surveillance technologies beyond visual cameras, and preventing the entry of unauthorized items. During the event, the system monitors disturbances, analysing human behaviour and environmental factors like gas leaks or potential threats. Post-event, it addresses resource constraints, and traffic management, and directs first responders efficiently. Education on sensor capabilities is emphasized, considering various backgrounds of users, and highlighting the need for diverse sensors to address blind spots like fires.
- Another participant suggested using a crisis management tool, incorporating sensor input for detection and alerting, and providing real-time information for prevention and protection. Video Analytics detects abnormal situations before and during events, including suspicious behaviour, weapons, and crowd movements. Additional components may include OSINT for detecting disinformation, noise sensors, and non-video crowd movement analysis. It anticipates minimal improvement needs for the proposed sensors/solutions, primarily focusing on integration. The use of OSINT (Open-Source Intelligence) and similar tools was proposed by other respondents too.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

- Various respondents proposed solutions through crowd management capabilities calibrated based on risk levels, associated with other detections that can be qualified in the context of the event.
- A solution that combines crowd event and movement detection per drone, personal enhanced alert, and real-time mass information was also mentioned.

Concerning the prioritised steps, the input from the market indicates that Assess/Follow and Detect/Alert could be tackled with audio surveillance, analysis, a designated alerting system, geolocation tools, and message broadcast to the general public.

6. Do you have knowledge of any suitable technology or combination of technologies that cover the use case "Terrorist attack at train station and surrounding area"? Can this technology or combination of technologies tackle one or more of the prioritised steps in order of importance: (1) Detect/Alert, (2) Assess/Follow, and (3) Prevent/Protect? Please elaborate.

The majority of respondents answered positively to the aforementioned question (see the stats above) thinking that their solution and technologies are suitable for the challenge in question.

Yes	7
No	3

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

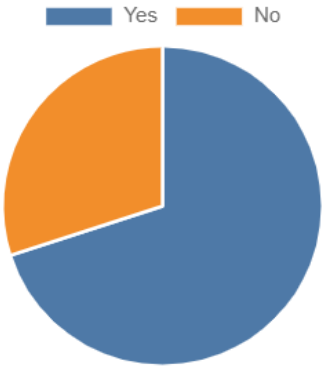


Figure 7.- Answers regarding technologies that can address scenario 3.

A summary of the answers received can be found below:

- A technology provider proposed a system for event security management involving three phases: pre-, during, and post-event, all integrated into one large system. Pre-event focuses on monitoring access, surveillance, and technology beyond visual cameras to prevent unauthorized entry. During the event, monitoring identifies disturbances and analyses behaviour, environmental factors, and potential threats. Post-event addresses resource allocation, directing first responders, and education on sensor capabilities, emphasizing the need for diverse sensors to address blind spots like fires.
- Another participant suggested a solution for the challenge in question through proper crisis management, integrating sensor input for detection and alerting, and providing information for prevention and protection specifically in the event of a terrorist attack. Video Analytics serves as the primary source of information, detecting abnormal situations before and during the attack, including suspicious behaviour, weapon detection, and crowd movement analysis. This real-time data aids stakeholders in managing public safety, identifying threats, and supporting crisis management efforts. Additionally, sound sensors may be considered to detect and classify specific sounds related to the attack and communicate them to the crisis management solution.
- The most common solution that was proposed related to video analytics and surveillance. It can combine multi-camera analysis along with tracking and identification or, alternatively, with audio surveillance along with a designated

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

alerting system, geolocation tools, and message broadcast to the general public.

Concerning the prioritised steps, the respondents indicated that their technological solutions could tackle – directly or indirectly – one or several of them.

7. If you were to develop the solution for the use case "Coordinated bomb and CBRN attacks during major sport events", how much time would you need for each of the three phases of the PCP: (1) solution design, (2) prototype development, (3) original development and testing of the solution?

Participants provided a time estimation for the development and deployment of the solution for the first use case including all the three PCP phases, highlighting the complexity and variability of the factors involved. Estimates varied depending on factors such as technology selection, solution scope, and site-specific requirements.

	Minimum Time Required	Average Time Required	Maximum Time Required
Phase 1: Solution Design	~ 1 month	3 - 4 months	6 months
Phase 2: Prototype Development	~ 4 months	7 months	12 months
Phase 3: Original Development and Pilot Testing	~ 3 months	5 months	10 months

Table 2.- Required time per PCP phase for use case 1.

A summary of the answers is provided below:

- One participant indicated that the estimated time for Phase 1 would be around three (3) months, for Phase 2 around six (6) to nine (9) months, and for Phase 3 around six (6) months.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

- The timeline offered by other participants was longer; for example, four (4) to six (6) months for the solution design phase, ten (10) to twelve (12) months for the prototype development, and six (6) to ten (10) months for the original development and testing – while some require a year for the whole process.
- Other participants suggested faster timelines with immediate results in Phases 1 and 2, or a minimal buffer time of one (1) to three (3) months for starting the prototype development, and a maximum of four (4) to six (6) months for the testing and original development.
- Finally, some respondents indicated that they already have the necessary technology at their disposal but require time to fine-tune the use cases and adjust the parameters according to the specifications of the potential PCP.

8. If you were to develop the solution for the use case "Concert venue chaos: disinformation – induced panic", how much time would you need for each of the three phases of the PCP: (1) solution design, (2) prototype development, (3) original development and testing of the solution?

Participants provided a time estimation for the development and deployment of the solution for the second use case including all the three PCP phases, highlighting the complexity and variability of factors involved (as stated in question 7).

	Minimum Time Required	Average Time Required	Maximum Time Required
Phase 1: Solution Design	1 – 2 months	4 months	6 months

Phase 2: Prototype Development	3 - 4 months	7 months	12 months
Phase 3: Original Development and Pilot Testing	3 - 4 months	6 months	10 months

Table 3.- Required time per PCP phase for use case 2.

A summary of the answers is provided below:

- One participant indicated that the estimated time for Phase 1 would be around three (3) months, for Phase 2 around six (6) to nine (9) months, and for Phase 3 around six (6) months.
- The timeline offered by other participants was longer; for example, four (4) to six (6) months for the solution design phase, ten (10) to twelve (12) months for the prototype development and another six (6) to ten (10) months for the original development and testing.
- Other respondents offered faster timelines with immediate results in Phases 1 and 2, or a minimal buffer time of one (1) to two (2) months for the commencement of the prototype development and a maximum of four (4) to six (6) months for the testing and original development.
- Finally, some respondents indicated that they already have the necessary technology at their disposal but require time to fine-tune the use cases and adjust the parameters according to the specifications of the potential PCP.

9. If you were to develop the solution for the use case "Terrorist attack at train station and surrounding area", how much time would you need for each of the three phases of the PCP: (1) solution design, (2) prototype development, (3) original development and testing of the solution?

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

Participants provided a time estimation for the development and deployment of the solution for the second use case including all the three PCP phases, highlighting the complexity and variability of factors involved (as stated in question 7).

	Minimum Time Required	Average Time Required	Maximum Time Required
Phase 1: Solution Design	1 – 2 months	3 months	6 months
Phase 2: Prototype Development	2 - 3 months	6 months	12 months
Phase 3: Original Development and Pilot Testing	~ 4 months	5 months	10 months

Table 4.- Required time per PCP phase for use case 3.

A summary of the answers is provided below:

- One participant indicated that the estimated time for Phase 1 would be around three (3) months, for Phase 2 around six (6) to nine (9) months, and for Phase 3 around six (6) months.
- The timeline offered by other participants was longer; for example, four (4) to six (6) months for the solution design phase, ten (10) to twelve (12) months for the prototype development and another six (6) to ten (10) months for the original development and testing.
- Other respondents offered faster timelines with immediate results in Phases 1 and 2, or a minimal buffer time of one (1) to two (2) months for the commencement of the prototype development and a maximum of four (4) to six (6) months for the testing and original development.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

10. If you were to develop the solution for the use case "Coordinated bomb and CBRN attacks during major sport events", could you indicate an estimated budget for the development and deployment of the solution? Please justify your answer.

Participants provided a range of estimates for the budget required to develop and deploy the solution, highlighting the complexity and variability of factors involved. Estimates varied depending on factors such as technology selection, solution scope, and site-specific requirements. Some respondents emphasized the need for comprehensive analysis before providing a precise estimate, while others outlined detailed breakdowns of costs for different project phases and components. Estimates encompassed expenses for personnel, subcontracting, materials, and testing, with considerations for equipment, infrastructure, regulatory compliance, and analytics.

	Minimum Estimated Budget	Average Estimated Budget	Maximum Estimated Budget
Phase 1: Solution Design	~ 100.000 - 125.000 euros	~ 525.000 euros	~ 1.5 million euros
Phase 2: Prototype Development	~ 100.000 - 125.000 euros	~ 740.000 euros	~ 1.5 million euros
Phase 3: Original Development and Pilot Testing	~ 100.000 - 125.000 euros	~ 1 million euros	~ 2 million euros

Table 5.- Required budget per phase for use case 1.

A summary of the answers is provided below:

- One participant indicated that the estimated budget for Phase would be around 400.000 euros, for Phase 2 around 1.250.000 euros and for Phase 3 around 2.000.000 euros. The aforementioned budget includes both video analytics and crisis management tools.

- Another respondent valued the efforts of its company at around 4.500.000 euros for the three phases.
- Others calculated the estimated budget based on the man-hours or days or the teams that would be involved in the PCP. This method of calculation along with the use of highly sophisticated technologies could raise the budget significantly.
- Ranging from 150.000 to 500.000 euros, another respondent indicated the convenience of better assessing the situation based on the needs and the circumstances before concluding on a fixed amount.
- Finally, a participant underlined that it would need around 200.000 euros for the development of the required solution, and around 500 euros for its deployment (per device) resulting in a cost of < 5€/m² of monitored surface. Therefore, it seems to prefer a cost per unit of surface valuation of its supplies and services, while the cost per unit of surface could be reduced depending on the exact scenario and the target level of measurements' accuracy.

11. If you were to develop the solution for the use case "Concert venue chaos: disinformation – induced panic", could you indicate an estimated budget for the development and deployment of the solution? Please justify your answer.

Participants provided a range of estimates for the budget required to develop and deploy the solution, highlighting the complexity and variability of factors involved. Estimates varied depending on several factors (see question 10).

	Minimum Estimated Budget	Average Estimated Budget	Maximum Estimated Budget
Phase 1: Solution Design	~ 10.000 euros	~ 580.000 euros	~ 1.5 million euros

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

Phase 2: Prototype Development	~ 10.000 euros	~ 800.000 euros	~ 1.5 million euros
Phase 3: Original Development and Pilot Testing	~ 10.000 euros	~ 995.000 euros	~ 2 million euros

Table 6.- Required budget per phase for use case 2.

A summary of the answers is provided below:

- One participant indicated that the estimated budget for Phase 1 would be around 400.000 euros, for Phase 2 around 1.250.000 euros and for Phase 3 around 2.000.000 euros. The aforementioned budget includes both video analytics and crisis management tools.
- Another respondent valued the efforts of its company at around 4.500.000 euros for the three phases of the PCP.
- A company underlined that the budget estimation needs to be linked to the number of audio surveillance infrastructure per location, ranging between 10.000 and 300.000 euros.
- Others calculated the estimated budget based on the man-hours or days or the teams that are going to be involved. This method of calculation along with the use of highly sophisticated technologies can raise the budget as high as 350.000 euros and in some cases even up to 1.000.000 euros.

12. If you were to develop the solution for the use case "Terrorist attack at train station and surrounding area", could you indicate an estimated budget for the development and deployment of the solution? Please justify your answer.

Participants provided a range of estimates for the budget required to develop and deploy the solution, highlighting the complexity and variability of factors involved. Estimates varied depending on several factors (see question 10).

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

	Minimum Estimated Budget	Average Estimated Budget	Maximum Estimated Budget
Phase 1: Solution Design	~ 10.000 - 50.000 euros	~ 415.000 euros	~ 1.8 million euros
Phase 2: Prototype Development	~ 10.000 - 50.000 euros	~ 556.000 euros	~ 1.8 million euros
Phase 3: Original Development and Pilot Testing	~ 10.000 - 50.000 euros	~ 625.000 euros	~ 1.8 million euros

Table 7.- Required budget per phase for use case 3.

A summary of the answers is provided below:

- One participant indicated that the estimated budget for Phase would be around 350.000 euros, for Phase 2 around 1.150.000 euros and for Phase 3 around 1.650.000 euros. The aforementioned budget includes both video analytics and crisis management tools.
- Another respondent valued the efforts of its company at around 5.500.000 euros for the three phases of the PCP.
- A company underlined that the budget estimation needs to be linked to the number of audio surveillance per location, ranging between 10.000 euros and 300.000 euros.
- Others calculated the estimated budget based on the man-hours or days or the teams that are going to be involved. This method of calculation along with the use of highly sophisticated technologies can raise the budget as high as 350.000 euros and in some cases up to 500.000 euros.

13. Can you provide any other recommendations regarding the three challenges?

A summary of the recommendations is provided below:

- A respondent noted that by using one central system that fact alone segments use cases and access into different areas for different individuals. It was mentioned that the three described use cases have the same core scenarios: pre-phase of the event and how to gather information, during the event and how to respond, and post-phase of the event and how to investigate.
- Another participant identified the need for cooperation between various agencies and responders as the weakest aspect during incidents that involve crowd management. Meanwhile, others agreed with this observation and suggested using hypervision and supervision tools for a better overview of the situation.
- One of the technology providers recommended testing generic existing solutions (with a TRL>7) to address the challenge.
- It was noted that the challenges require different skills, and it may be difficult to build consortiums including all the required aspects (video analytics, CBRN, milliwaves, 3D modelization tools, etc.) to address all the functionalities of the challenges due to PCP rules (one company in only one consortium). It might be more efficient for some sensors to open parallel calls, e.g. to assess their efficiency while asking the main consortiums to integrate those providers in their platform.
- Furthermore, examining the crisis management topic introduced by one of the technology providers standard-setting, requirements about Open APIs as well as documentation sharing seem to be essential for the smooth cooperation of the various stakeholders and actors in case of an emergency.
- Finally, there was a recommendation concerning video analytics where compliance must be adopted due to the EU regulatory framework, to focus on core processes regarding the challenges and to also focus on a limited number of sensors (e.g. type or nature).

3.3.2 The State-Of-The-Art Analysis

1. Do you think there is room for technological development beyond the state of the art? Please explain.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

Several technological developments were outlined by the participants. The input provided by the companies confirms that there is room for innovation.

A summary of the answers is provided below:

- A participant confirmed that there is room for aggregation of an entire system and the connection between the signals and components which in turn would be beyond the current state of the art. Focusing and interpreting all the different systems connected into a central platform from the number of sensors and software required for this would need implementation work. Setting up user groups and rights will have to be managed.
- For crisis management, it was claimed that a map-based multi-media communication and AI-based decision-support tooling, considering all sources of information, are innovative compared to the SOTA analysis.
- For video analytics, it was foreseen that new development can focus on various aspects of this field such as the enhancement of sensors and detectors of objects and the crowd combined with the most suitable and contemporary AI models.
- It was also highlighted that, although some solutions are available for crowd management (detecting unusual crowd movements, panic, violence, fight, etc.), currently it is not possible to "play" with real-life situations in public space. In addition, detecting drones in complex environments is also difficult due to a lack of training data and further development would be required.
- A proposed solution would be to add edge processing and smart audio analysis with artificial intelligence innovating and developing custom software.
- The need to collect specific datasets, along with the development of miniature gas detectors, explosive and bacteriological threat detection tools and a multi-threat CBRN detector technology, leaves room for further innovation.
- All the technological building blocks for managing crowd alerts in terms of qualification/information are available. However, their use in a highly resilient and efficient way, with the coordination of players, has not yet been developed.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

2. What kind of solutions or developments would you propose?

Concerning specific solutions or developments to be implemented, a summary of the answers is provided below:

- One of the proposed solutions includes a system that would allow the user to obtain the correct and relevant information at the correct time. It is not a new technology that needs to be developed, but a result of the aggregation of technology. The main challenge would be how to acquire information from the real world and include it in the new systems that are designed for a separate group of individuals.
- Regarding crisis management, the proposed solutions aim to enhance external risk assessment and real-time monitoring of events, alongside integrating collaborative tools with map-based activities and multimedia communications. These solutions would be complimented by AI support and analytics tools.
- In the field of video analytics, proposed advancements include a new object detector for weapons and law enforcement equipment, along with AI models for extracting relevant data, analyzing crowd movements, identifying suspicious behaviors, and integrating mobile cameras and drones. Additionally, new interfaces and IoT devices are being integrated to improve on-the-field data quality, along with dedicated connectors between video analytics and crisis management systems for seamless integration and mobile app usage.
- Several innovative technologies were mentioned as tools for the provision of practical solutions in the three scenarios, such as detection of unattended items, drone detection, real-time crowd/video analysis, the use of a hypervision platform, mapping and communication, the further development of LIDAR or similar sensors, social network and dark web screening, social media management, proper use of communication tools to address issues linked to the general public and tracking including facial recognition.
- A pilot of an existing solution to evaluate the need for development (if any) for each scenario, followed by the specification of the roadmap to the final models, was proposed by another respondent.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

- Some respondents suggested adopting a global approach that would cover the needs of the different actors involved in the events, while others proposed a smart audio analysis with AI.
- A technology that uses a network of sensors with central data treatment software to create an early warning system, with attack monitoring and mitigation proposals, was also discussed.
- There were proposals for the development of a miniaturized gas detector and working against CBRN threats to protect the general public.
- Another aspect to consider would be a web-based analytical application for exercising crisis management and response, along with a computer platform for raising crisis situational awareness and training decision-makers by role playing in simulated situations.
- Another proposal was a Decision Support System built on a software platform for the development of data-driven knowledge-based decision support systems and multi-criteria analysis tools (Decision Support Framework).

3. Do you know the Technology Readiness Level (TRL) of those solutions/developments? If yes, please indicate them below:

Overall, the TRL of the solutions and developments proposed by the technology providers differs significantly due to the unique nature of each technology. Nonetheless, the spectrum of TRL starts from TRL 2, reaching up to TRL 9.

A summary of the answers is provided below:

- Technology for Crisis Management: Overall, TRL 5 per function requested. Nevertheless, there is a need to assess the TRL in case of integration of different components (internal and external).
- Technology for Video Analytics: The maturity of the video functionalities as presented in questions 14 and 15 is at TRL 5. The addition of other sensors can

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

present high variability between the different components of the solution classifying it from TRL 3 to 8 with an overall TRL 5.

- Unattended item detection technology: TRL 7.
- Drone detection technology: TRL 4.
- Real-time crowd/video analysis technology: TRL 5.
- Hypervision platform, containing mapping and communication: To be developed for specific needs.
- Intervention plan suggestions: To be developed for specific needs.
- LIDAR or some other sensors: TRL 2.
- Social network and dark web screening - TRL 8.
- Social media management: TRL 7.
- Communication tools to the public: TRL 4.
- Tracking including facial recognition: TRL 4.
- Laboratory: TRL 7.
- Serious Gaming Platform: TRL 9.
- Decision Support Framework: TRL 5.

4. Can you identify any patents or standards that are relevant to the challenge? If yes, please indicate them below:

The majority of the respondents answered negatively to this question. However, one of them highlighted that the final solution needs to consider the GDPR and EDXL framework of standards and that the exploitation and improvement of pre-existing patents are crucial for addressing the presented challenges.

5. Are you aware of any patents that may constitute a barrier for you to deliver a solution in the envisaged PCP procurement? If yes, please indicate them below:

The participants who filled in the questionnaire were not aware of any patent that could potentially hinder their solution design and delivery in the context of the envisaged PCP procurement.

One respondent mentioned the third-party drone takeover and recovery regulations as a potential barrier.

3.3.3 Miscellaneous

1. What information do you still need in order to make a good plan of action for the development and/or implementation of solutions suitable to address the challenge?

A summary of the answers is provided below:

- It would be crucial for each selected technology provider to know which companies are involved in the solution development in order to ensure that their approaches are harmonized and fully integrated into the global solution, especially in the software upper layer of the solution.
- From an overall point of view, technology providers requested clear information on the list of the use cases that need to be addressed, a typical RACI matrix with the main stakeholders for each phase of the event (Prevent/Detect/Access/Resolve/Post-Investigate), if possible categorization of the stakeholders, as well as the organization and establishment of relationships in place with regulators in each country where the respective solution will be developed.
- Specific information on the field of Video Analytics, such as a typical inventory of the quality of the infrastructures that will be used during the different phases (for example 500 cams with an expected 70% of average/good quality, 10% of bad quality that will be changed by new equipment, and 20% of bad quality that will remain).
- Information about the different systems (existing or not) in which the solution will be implemented and how to connect each other to obtain optimal results.

- Detailed functional requirements, in particular the rank (required, optional) of each feature to estimate if we could build a consortium with no more than three entities.
- Detailed specifications by scenario, with the priority of each one of them, as well as the interface requirements for integration of the models made available and/or developed.
- Details on gas threats that would be of interest for public safety protection and if they constitute a point of interest in the context of this project.
- According to another respondent, start-ups look for funding opportunities above all, hence a minimum level of commitment and interest from the side of the public buyers would potentially motivate the suppliers to speed up the development and/or implementation of solutions suitable to address the selected challenge.
- Information about environmental and network description specifications based on the project's objectives.

2. Do you have specific requirements to achieve the functionalities that SHIELD4CROWD should take into account? If yes, please indicate them below:

Many respondents declared that they do not have any specific requirements to achieve the functionalities for the future PCP. A summary of the answers is provided below:

- One respondent underscored that it should be informed about which companies would be involved in the potential solution development to contact them and ensure that their approaches are harmonized and fully integrated into the broader framework of the project (e.g. software upper layer of the potential solution).
- Another company requested from the Consortium the following information to guide the Contactor in the solution design phase: a) defining to what extent

each stakeholder is ready to accept changes and adaptations in its way of operating, b) defining to what extent some processes cannot change due to legal and regulatory limitations or will encompass a certain level of delay being "too slow" from a temporal compatibility perspective in conjunction with the project's schedule, and c) identifying and indicating, if available, open APIs to connect properly all the different components.

- It would be essential to be provided with detailed requirements about data collection.
- Lastly, it was suggested that Phase 2 of the PCP needs to be long enough (around 12 months) to enable enough iterations of the solution development and its iterative assessment.

3. What are the risks associated to the development and implementation of a solution that tackles the functional needs of SHIELD4CROWD?

A summary of the answers concerning potential risks is provided below:

- Privacy concerns.
- Heterogeneity in the digital ecosystems and between the countries that will be involved and interconnected in the context of the project may cause some interoperability and harmonization issues.
- Differences in command chains and procedures in the participating regions and organizations may pose difficulties in the proper implementation of the developed solution.
- Legal conformity and understanding the "call to action" and "doubt-dispelling" approaches to the technology.
- Risks related to project management, such as project failure or mistakes during the testing and validation of the solutions. Local testing needs to be carefully prepared and repeated several times according to strict protocols.
- Risk of vandalism of the deployed equipment. A safe and discrete design would reduce this risk.
- Deployment costs.

4. Do you have any suggestions and/or remarks?

The majority of respondents did not have any further suggestions or remarks addressed to the SHIELD4CROWD Consortium at the time.

Only one respondent mentioned the need to consider cyber resilience and critical communications. Cybersecurity should be an integral part of the overall process, while each component or element of the solution should include parameters to safeguard it. Furthermore, it underscored that efficient and unhindered communication between stakeholders during a crisis is vital. Therefore, any potential shutdown or saturation of the communication channels would render a potential solution less effective, if not completely useless.

4. The follow up PCP

The SHIELD4CROWD Consortium will prepare and submit an application in the upcoming months to receive funding from the EC to conduct a PCP. The future PCP will focus on one of the three use cases presented during the OMC, or a combination thereof that covers the needs of the different PTOs and security practitioners.

The future PCP is expected to be launched in early 2026.

5. Conclusions

The Open Market Consultation (OMC) conducted within the framework of SHIELD4CROWD was an exceptional opportunity to interact with market operators and receive their feedback about the three use cases presented, as well as other

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

procedural aspects. The level of participation of technology providers from different European countries revealed great interest from the market in this project.

The analysis of the responses to the twenty-two (22) questions posed through the Request for Information (RFI) questionnaire and the feedback received during the OMC event revealed several key insights. The OMC showed that the market is characterized by a diverse range of technological solutions and expertise aimed at addressing the challenges associated with the use cases on a) "Coordinated bomb and CBRN attacks during major sport events", b) "Concert venue chaos: disinformation – induced panic", and c) "Terrorist attack at train station and surrounding area". The technology providers indicated a wide array of methodological approaches (e.g. detection, prevention, etc.) and technological means at their disposal, ranging from Aggregated Information Systems (AIS) and Crisis Management Tools to advanced visual/audio analytics that harness AI capabilities. Furthermore, additional innovative and emerging technologies were proposed, such as standard drones, sensors and surveillance infrastructure, hypervision platforms, AI models for behavioural analysis and light detection and ranging (LIDARs) systems).

The assumption of SHIELD4CROWD that there is interest and capacity within the market to develop and implement innovative solutions for the three use cases was largely validated during the OMC. Since the average TRL of the proposed solutions is 5 - 6, it can be concluded that there is room for further R&D to develop a solution that covers the public buyers' needs, enhancing the safety of public spaces and crowd management in crisis situations.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

Annex I. Agenda of the OMC webinars

OMC webinar in English

Online Event

2 April 2024 | 10:00 to 11:30h CET

Location: Microsoft Teams

Hours	Topic	Presenter
10:00 - 10:20	**Introduction to the S4C project and PCP**	SNCF
10:20 - 10:40	**Presentation of the 3 use cases**	SNCF
10:40 - 10:50	**Presentation of the state of the art analysis**	SAFE
10:50 -11:05	**OMC objectives and activities**	CORVERS
11:05 -11:20	**Open discussion**	All participants
11:20 -11:30	**Closure**	SNCF

OMC webinar in French

Online Event

3 April 2024 | 10:00 to 11:30h CET

Location: Microsoft Teams

Hours	Topic	Presenter
10:00 - 10:20	**Introduction to the S4C project and PCP**	SNCF / MIOM
10:20 - 10:40	**Presentation of the 3 use cases**	SNCF
10:40 - 10:50	**Presentation of the state of the art analysis**	SAFE
10:50 -11:05	**OMC objectives and activities**	SNCF
11:05 -11:20	**Open discussion**	All participants
11:20 -11:30	**Closure**	SNCF

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

OMC webinar in Italian

Online Event

4 April 2024 | 10:00 to 11:30h CET

Location: Microsoft Teams

Hours	Topic	Presenter
10:00 - 10:20	**Introduction to the S4C project and PCP**	DIGINNOV
10:20 - 10:40	**Presentation of the 3 use cases**	DIGINNOV
10:40 - 10:50	**Presentation of the state of the art analysis**	DIGINNOV
10:50 -11:05	**OMC objectives and activities**	DIGINNOV
11:05 -11:20	**Open discussion**	All participants
11:20 -11:30	**Closure**	DIGINNOV

OMC webinar in Slovakian

Online Event

4 April 2024 | 12:00 to 13:30h CET

Location: Microsoft Teams

Hours	Topic	Presenter
10:00 - 10:20	**Introduction to the S4C project and PCP**	MVSR
10:20 - 10:40	**Presentation of the 3 use cases**	ISEMI
10:40 - 10:50	**Presentation of the state of the art analysis**	MVSR
10:50 -11:05	**OMC objectives and activities**	MVSR
11:05 -11:20	**Open discussion**	All participants
11:20 -11:30	**Closure**	MVSR

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

OMC webinar in Spanish

Online Event

5 April 2024 | 10:00 to 11:30h CET

Location: Microsoft Teams

Hours	Topic	Presenter
10:00 - 10:20	**Introduction to the S4C project and PCP**	ESMIR / CORVERS
10:20 - 10:40	**Presentation of the 3 use cases**	ESMIR
10:40 - 10:50	**Presentation of the state of the art analysis**	ESMIR
10:50 -11:05	**OMC objectives and activities**	CORVERS
11:05 -11:20	**Open discussion**	All participants
11:20 -11:30	**Closure**	ESMIR

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

Annex II. Agenda of the OMC event in Warsaw

Hybrid Event

15 May 2024 | 9:00 to 16:15h CET

Location: Centrum Szkoleniowe Wspólna, Wspólna 56, 00-686 Warsaw

Hours	Topic	Presenter
9:00 – 09:15	**Participants registration and welcome coffee**	
9:15 – 09:30	Introduction to the S4C project	SNCF
9:30 – 09:45	Presentation of the 3 use cases	SNCF
9:45 – 10:55	Presentation of the state-of-the-art analysis	SAFE
10:55 – 11:15	Introduction to PCP + OMC objectives and activities	CORVERS
11:15 – 11:45	Coffee break	
11:45 – 12:15	Workshop challenge 1 "Coordinated bomb and CBRN attacks during major sports events"	All participants
12:15 – 12:45	Workshop challenge 2 "Concert venue chaos: disinformation – induced panic"	All participants
12:45 – 13:15	Workshop challenge 3 "Terrorist attack at train station and surrounding area"	All participants
13:25 – 13:30	Closure	SNCF
13:30 – 14:30	Lunch break	
14:30 – 14:35	Introduction to the matchmaking session	CORVERS
14:35 – 15:15	Presentation by suppliers of their company and capabilities	All participants
15:15 – 16:00	Matchmaking session	All participants
16:00 – 16:15	OMC closure	CORVERS

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

Annex III. E-pitching sessions summary

Introduction

Along with the OMC, and to complement the market analysis, SHIELD4CROWD carried out a series of e-pitching sessions on the 15th, 16th, and 17th of April 2024. Each day of e-pitching sessions was dedicated to one of the three use cases of the project concerning the protection of public spaces in EU cities against security threats related to crowd management: 1) Coordinated bomb and CBRN attacks during major sports events, 2) Concert venue chaos: disinformation – induced panic and 3) Terrorist attack at train station and surrounding area.

A total of fifty (50) technology providers from six different countries (France, Spain, Greece, Italy, Poland, and Slovakia) participated in the e-pitching sessions; eighteen (18) on the first day (Challenge 1), twelve (12) on the second day (Challenge 2), and twenty (20) on the third day (Challenge 3). During the sessions, they presented their respective companies, the existing solutions, and their R&D efforts and capabilities. Some technology providers proposed similar solutions based on their expertise for multiple challenges. Therefore, unique solutions per challenge can be identified, yet there are overarching ones too.

While some of the presented solutions (even up to TRL 9 according to some technology providers) could tackle aspects related to SHIELD4CROWD scenarios, none of them seem to cover all the functionalities related to a specific challenge. The potential for further developments, the adjustments of pre-existing solutions based on each challenge's specifications, and the combination of technologies seem promising for the future PCP challenge, considering the maturity of many solutions (at TRL 4-6) and the expected R&D plans.

Challenge 1: Coordinated bomb and CBRN attacks during major sports events (15 April 2024)

In scenario one, the SHIELD4CROWD Consortium has decided to prioritise the following three steps: (1) Detect/Alert, (2) Assess/Follow, and (3) Resolve.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

The summary of the solutions proposed by the technology providers is provided below:

- Modelling and predicting blast consequences in an urban environment while determining injury and lethality zones, both outdoor and indoor. The solution can be combined with pre-processing tools for data import from Building Information Modelling sources (TRL 5).
- Modelling the Chemical/Biological (C/B) release and consequences based on fast-running transient source term models.
- Use of Unmanned Aerial Vehicle (UAV) for live video integrated on top of 3D maps and adjusted to the particularities of the urban environment via photogrammetry.
- Combination of crisis management tools (with multiple Application Programming Interfaces (APIs) for interoperability and connectivity with third-party components along with mapping components and multi-media communications) and video analytics (through object and crowd movement detection via Artificial Intelligence (AI) models and the improvements of existing detectors). This is based on components integration and adjustments from TRL 5 up to TRL 9.
- Disaster recovery plan for continuous radio broadcasting to inform the population through reliable real-time satellite transport for eight stereo programs in low bitrate (<2 Mbits/s).
- Deployment of a powerful pre-existing 360° situational awareness and security platform with the integration of new scenarios adjusted to the occasion while using CBRN sensors, thermal imaging technologies, and drones as data sources.
- An AI-based information-sharing mechanism that facilitates real-time situation awareness by analysing crowd movements, enabling efficient communication and coordination among Law Enforcement Agencies (LEAs) and Frontline Responders (FRs).
- Multimodal fusion and correlation techniques to conduct a risk assessment, aiding decision-support processes while visualizing layered zones based on the distribution of networked sensors for observation, notification, and neutralization purposes.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

- Omnibotic solution (consisting of an autonomous drone and a drone box) with the ability to patrol effectively over large areas, enhancing surveillance, enabling rapid and cost-effective verification in case of triggered alarms (expanding the use of rolling robots), potential improvements on the detection systems and algorithms enhancing accuracy and versatility.
- Use of Large Language Models (LLMs) and AI Agents for Information and Knowledge Management Optimization thanks to traits such as data volume and diversity, dynamic visualization and analysis, and a high level of customization and adaptability. It has the potential for specialization in geopositioned data permitting operational intelligence, real-time information and therefore resolution through data.
- Smart sensors and, specifically, the deployment of radiological beacons for threat monitoring that provide real-time data, quick threat alert, and tools to secure first responders intervention. It would be possible to add chemical capabilities to the sensors and development of a miniature and low power Field Asymmetric Ion Mobility Spectrometry using Micro-Electro-Mechanical Systems for the detection of explosives and even gas leaks and industrial incidents.
- Detection of chemical threats by using heterogeneous sensors, dedicated translators, and sensor nodes with capabilities of classification and identification of threats (TRL 8). It would be possible to integrate radiological, biological, or another type of sensors based on the specifications of the project (TRL 6).
- Electronic Logbook and Operational Management Software ensuring traceability, security event management, and inter-service information exchange functioning as a safety hypervisor as well as a collaborative platform to manage and share information in real-time and helping in decision-making and resources management (TRL 9).
- Advanced drone exploitation with the possibility of detecting and tracking all types of targets, high-level of interconnection of several systems with a series of other features such as possible connection to a control command (APIs) and several installation configurations (fixed or mobile) coming along with it.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

- Perimetrical protections, namely free-standing barriers and speed bumpers with road blocker systems with the potential of developing further similar products and accessories through Computer-Aided Design (CAD) software.
- Enhanced radiological mapping system to serve a global public event supervision ecosystem through specialized CBRN tools for the real-time detection and communication of measurement data disseminating the information on multiple levels. Potential development of ultra-light dose rate probes for micro-drones and nuclide identification probes adapted for the last generation of CBRN Unmanned Aerial Vehicles (UAVs) and Unmanned Ground Vehicles (UGVs).
- Specialized clothing including gloves, cartridge masks, hoods, and overboots – among others – to ensure personal protection in cases of CBRN attacks with additional protective equipment related to decontamination or even medical evacuation solutions. There is room for further innovations in the field of functionalized textiles, new protective materials, and decontamination solutions all encompassed under a broader network of interconnected and enhanced technologies against CBR attacks.
- Exploiting active standoff detectors for the detection of CBRN agents, and monitoring of the situation post-attack with the potential incorporation of AI and automatization solutions with sharing data as well as user-friendly software.
- Adoption of simulation-based decision/support solutions for large crowds, public spaces, and critical infrastructures security based on immersive serious gaming, event planning support, and virtual security strategy assessments. Several R&D features may follow involving indicatively AI-based training of crowd models, live what-if simulations and post-event analysis.
- Detection enhancement and focus on identification based on multiple sensor fusion from radiofrequency scanners and radar to AI/ML image processing with the potential to include in this ecosystem means of alert/notification and hard-core intervention (e.g. Electronic Warfare mitigation).
- A new generation of AI solutions for the detection of objects, individuals, and crowds along with other characteristics from crowd density to agitation. It would be possible to generate new models or re-training the existing ones

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

offering room for flexibility and parametrization based on a case-by-case approach.

Challenge 2: Concert venue chaos: disinformation – induced panic (16.04.24)

In scenario two, the SHIELD4CROWD Consortium has decided to prioritise for this use case the following four steps: (1) Assess/Follow, (2) Prevent/Protect, (3) Resolve, and (4) Detect/Alert.

The summary of the proposed solutions is presented below:

- Combination of crisis management tool (with multiple APIs for interoperability and connectivity with third-party components along with mapping components and multi-media communications) and video analytics (through object and crowd movement detection via AI models and the improvements of existing detectors). This is based on components integration and adjustments from TRL 5 up to TRL 9.
- Use of the local entertainment audio system for public announcements prioritising audio over Internet Protocol (IP) public address system, while adopting a network hypervision approach.
- Plausible solution through the acquisition of reliable hardware (e.g. ruggedized telecommunication devices) with custom-made services and dedicated support – multi-mission smartphones with improved connectivity and innovative features and accessories. There is room for the development of additional features such as geolocation of the available units in the area through Mission Critical services (MCX) dispatcher, deployment of forward command posts and media monitoring on site, voice communication flows enhanced by images and videos, etc.).
- Use of a powerful pre-existing 360° situational awareness and security platform evolved with the incorporation of Dynamic Risk Assessment and the capacity to process Weak Signals.
- AI-based information-sharing mechanism that facilitates real-time situation awareness by analysing crowd movements, enabling efficient communication and coordination among LEAs and FRs.

- Social Media Security Threat Detection through the extraction of relevant information from social media, performing a sentiment analysis.
- Use of drones/captive drones/swarm drones as a data source and classification of the threat type and level via video analytics.
- Deployment of dedicated software for crowd management which can calculate several factors from the speed and direction of the public to the perception of abnormal events. There is potential for the development of new features like enabling natural language requests on video streams and/or natural language scenarios and enhancement of already existing functions.
- A system that offers a constant overview of an entire perimeter using video analytics, including optic sensors and central analytical platforms, combined with live streams from drones, car or body cameras and through accurate automatic detection and activation of prepared processes for specific events increases the speed of response.
- Use of Geospatial Intelligence (GEOINT) technologies through a system that analyses and visualises key locations (such as buildings, stadiums, or train stations), identifying exits, main lanes, and congestion points, while generating mobile and vision-based heatmaps to monitor crowd density and movement in a contactless manner.
- Integrating spatial behaviour models that predict individual movements and developing AI-driven algorithms to generate and disseminate real-time evacuation instructions tailored to the location and type of threat. The instructions are continuously updated based on crowd movement and spatial behaviour models.
- Use of LLMs and AI Agents for Information and Knowledge Management Optimization thanks to traits such as data volume and diversity, dynamic visualization and analysis and a high level of customization and adaptability. There is potential for specialization in geopositioned data permitting operational intelligence, real-time information and therefore resolution through data.
- Electronic Logbook and Operational Management Software ensuring traceability, security event management and inter-service information

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

exchange functioning as a safety hypervisor as well as a collaborative platform to manage and share information in real-time and helping in decision-making and resources management (TRL 9).

- An innovative ecosystem that combines sensor fusion and data (from optic sensors, lidars and radars) with 3D digital twins, providing accurate simulations, flow management, spatial intelligence and a network of robust and secure communication. It would offer optimal chances for predictive and post-analysis leading to efficiency and optimization.
- A new generation of AI solutions for the detection of objects, individuals and crowds along with other characteristics from crowd density to agitation. It would allow to generate new models or re-training the pre-existing ones offering room for flexibility and parametrization based on a case-by-case approach.
- Adoption of simulation-based decision/support solutions for large crowds, public spaces and critical infrastructures security based on immersive serious gaming, event planning support, and virtual security strategy assessments. Several R&D features may follow involving indicatively AI-based training of crowd models, live what-if simulations and post-event analysis.
- Developing an innovative approach for interacting with intelligent video analytics, ensuring adaptability to evolving work environments, enhancing organizational control over next-generation AI capabilities, and advancing the TRL of density estimation, crowd movement detection, and unattended luggage detection in high-density conditions.
- Developing frugal and optimized AI models to reduce power consumption for efficient large-scale operations, and leverage AI indicators to create robust panic situation detection and prevention tools.

Challenge 3: Terrorist attack at train station and surrounding area (17 April 2024)

In scenario three, the SHIELD4CROWD Consortium has decided to prioritise for this use case the following three steps: (1) Detect/Alert, (2) Assess/Follow, and (3) Prevent/Protect.

The summary of the proposed solutions is presented below:

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

- Reliable and secure processing streaming and monitoring of IP audio streams along with the simultaneous delivery of multiple priorities audio programs to different sites or zones, while always complying with multiple technical and operational requirements.
- Deployment of computer vision software for real-time analysis with AI features that are non-biased and accurate, simply deployed on existing Closed-Circuit Television (CCTV) infrastructure and capable of examining and assessing the relevant environment. This may be accompanied by a smart tool with Digital Twins technology offering a collaborative and decisional solution to enhance security on site and foster teams' collaboration (e.g. first responders).
- Combining pre-existing space-derived magnetic measurement and modelling tech with crowd sensing neural network (TRL 9) to ensure the security of areas from weapons using a discrete and safe method alleviating security personnel and eliminating the need for control centres.
- Ensuring the proper development and integration of complementary software platforms, while guaranteeing the adequate level of cybersecurity in the use of AI such as supervised algorithms and anomaly detection.
- Use of UAV for live video integrated on top of 3D maps, but adjusted in the intricacies and uniqueness of an urban environment via photogrammetry
- Utilization of a powerful pre-existing 360º situational awareness and security platform and its extended capabilities for automated actions particularly concerning sound detection (e.g. shouts, shooting, etc.) and threat type and level through video analytics.
- Social Media Security Threat Detection through the extraction of relevant information from social media, performing a sentiment analysis.
- Application of dedicated software for crowd management able to calculate several factors from the speed, direction, and flow of the public to the perception of abnormal events varying from panic to firearm detection.
- Implementing the aspects of an innovative detection and information-oriented ecosystem combining personalized alerts focusing on keeping the general public informed in case of unusual events. This may be accompanied by

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

geofenced mass notification leaving room for further adjustments such as stronger APIs or an AI panic analyser.

- Utilization of a crisis communication platform with ingrained features such as real-time alerts to the general public and the coordinated response teams, provision of safety instructions, information about the crisis in the surrounding area, and more filtered through a command centre for the proper management of the situation. Customization is possible as well as map layers from various data sources.
- Online environment for modelling and simulations of critical infrastructures, real-life scenarios analysis, cascading effects consequences, and other factors (TRL=7) – potential adjustments and customization are possible for each separate case
- A computer platform for creating and running role-playing games that allows proper training of tactical decision-making and the overall improvement of situational awareness (TRL 9). Potential adjustments and customization are possible for each separate case.
- Electronic Logbook and Operational Management Software ensuring traceability, security event management, and inter-service information exchange functioning as a safety hypervisor as well as a collaborative platform to manage and share information in real-time and helping in decision-making and resources management (TRL 9).
- The exploitation of stereo-vision technologies via 3D camera detection, based on the human vision principle, and biometric analysis via AI for facial recognition and identification to provide overview and control over a potential terrorist attack.
- Integration of an AI platform offering rapid and precise analysis of both online and archived video streams, allowing customization with customer-specific datasets while including advanced reporting, alerts, and notification features. Potential interoperability with other systems and ensuring a centralized remote configuration and monitoring of geographically distributed installations of cameras underscores a high level of flexibility of the solution.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171

- An innovative ecosystem that combines sensor fusion and data (from optic sensors, lidars, and radars) with 3D digital twins that provide the opportunity for accurate simulations, flow management, spatial intelligence, and a network of robust and secure communication offers optimal chances for predictive and post analysis leading to efficiency and optimization.
- A new generation of AI solutions for the detection of objects (e.g. abandoned cars, firearms, etc.), individuals, and crowds along with other detection characteristics from crowd position and injury status of people to interpreting agitation. The possibility of generating new models or re-training the pre-existing ones. offering room for flexibility and parametrization based on a case-by-case approach.
- Simulating scenarios of given threat levels, and their probability and performing the analysis of their severity or potential impact allows for the preparation of the most suitable strategy and the further adoption of appropriate measures a priori.
- The deployment of an AI-powered computer vision platform for real-time analysis designed for critical infrastructure supervision, rendering any camera into an intelligent monitoring tool that ensures accurate detection of the safety of public places and the management of operations, people and vehicle flow. There is room for development of new applications.
- Benefiting from video analytics in conjunction with an in-depth and accurate flow analysis platform to improve operational efficiency with advanced counting features delivering unprecedented accuracy and efficiency to transform the way data is managed and analyzed.

This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101121171