SHIELD
PCP

Open Market Consultation Report

Report on the Open Market Consultation for the future Pre-Commercial Procurement of R&D services in the field of protection of public spaces and crowd management

Funded by the European Union

Disclaimer

Copyright notice

Abbreviations and acronyms

EC	European Commission
EU	European Union
GDPR	General Data Protection Regulation
HE	Horizon Europe
H2020	Horizon 2020
IPRs	Intellectual Property Rights
LEAs	Law Enforcement Agencies
M	Month
R&D	Research and Development
RFI	Request For Information
TRL	Technology Readiness Levels

Contents

Table of Figures

1. Executive summary

This report presents the results of the Open Market Consultation (OMC) carried out in the framework of the SHIELD PCP project (Security Harmonised Innovation for Enhanced Law Enforcement Capacities in Dynamic Crowd Protection). The OMC aimed to validate the preliminary state-of-the-art analysis, test the feasibility and attractiveness of the envisaged Pre-Commercial Procurement (PCP), and collect structured feedback from technology providers and other stakeholders on the SHIELD PCP challenge, pilots and requirements.

The consultation combined three main strands of activity: (i) a series of multilingual online webinars organised between 27 and 29 January 2026, (ii) a hybrid OMC event held in Paris from 25 to 26 February 2026, and (iii) a written Request for Information (RFI) questionnaire disseminated via the EU Survey platform. Across these activities, 189 stakeholders registered to participate, representing 11 countries and a mix of SMEs, mid-caps, large organisations, universities and research organisations, and other entities. In terms of organisational profile, 97 registered participants were SMEs, 48 large organisations, 6 mid-caps, 13 universities or research organisations and 25 from other types of entities.

The webinars provided an opportunity to present the SHIELD PCP context, the three priority pilots (panic at a football stadium, drone attack on match day, and multi-actor coordination after a massive knife attack in a train station), and the high-level functional and non-functional requirements, while also enabling real-time interaction through Q&A and live polls. The Paris event complemented this with a full-day programme combining plenary presentations, an interactive session and structured matchmaking. In total, 54 technology providers participated in the OMC hybrid event in Paris (85 participants in total when including consortium members and members of the User Observatory Group (UOG)), of whom 20 technology providers attended in person (45 participants in total with consortium members and UOG members) and 34 technology providers joined online (40 participants in total with consortium members and UOG members). Participants were introduced to the SHIELD PCP rationale, pilots, PCP phases and budget; received a detailed presentation of the state-of-the-art analysis and OMC objectives; and took part in an interactive discussion on requirements and technical approaches, followed in the afternoon by supplier pitches on company capabilities and a dedicated matchmaking session between technology providers and public buyers.

The RFI questionnaire gathered structured information on suppliers' profiles, relevant solutions, technology readiness levels (TRLs), foreseen IPR strategies, and views on legal, ethical and operational constraints. In total, 49 responses were received. The respondent base was dominated by SMEs and start-ups, while also including large companies, research organisations/universities, private organisations and one respondent selecting another category. In geographical terms, responses came from six countries, with the largest shares from Spain and France, followed by Italy, Greece, Slovakia and Belgium.

Overall, the OMC confirmed strong market interest in the future SHIELD PCP, a clear preference for modular and interoperable solutions, and broad availability of relevant technology building blocks, while also showing that substantial innovation is still needed in areas such as advanced crowd analytics, AI-supported decision-making,

multi-source data fusion, and legally and operationally robust multi-agency deployment. The feedback collected through the activities, and in particular through the detailed responses to the RFI questionnaire, provided important insights for the preparation of the future PCP procurement. While respondents generally confirmed the relevance of the SHIELD PCP challenge and the feasibility of developing innovative solutions, several topics emerged across the answers that may require further clarification or consideration when designing the procurement approach.

First, many respondents emphasised the importance of modular and interoperable architectures, highlighting that the envisaged solution should allow the integration of specialised components developed by different providers. Suppliers frequently indicated that open interfaces, standardised APIs and the ability to integrate with existing command-and-control, communication and sensor infrastructures will be essential for the successful deployment of solutions in real operational environments. This feedback supports a procurement approach that encourages modular innovation and avoids overly restrictive solution architectures.

Second, respondents repeatedly underlined the complexity of integrating heterogeneous data sources, sensors and analytics tools across multiple agencies and operational environments. Several answers pointed to interoperability with legacy systems, cross-agency data governance and semantic interoperability as important challenges. These observations suggest that the PCP may need to place particular emphasis on integration capabilities, open standards and data-governance mechanisms to ensure that developed solutions can operate effectively in multi-agency contexts.

Third, a number of responses highlighted legal, ethical and regulatory considerations related to the use of advanced sensing, analytics and artificial intelligence in public-space security contexts. Respondents referred in particular to GDPR compliance, transparency and accountability of AI-supported decision-making, and the need to ensure that surveillance or behavioural analysis technologies are deployed proportionately and in accordance with EU legal frameworks. These aspects will therefore need to be carefully reflected in the definition of technical requirements and evaluation criteria for the future PCP.

Fourth, suppliers frequently indicated that the most resource-intensive part of the development process is expected to be the integration and prototyping phase. Both the indicative timelines and the budget estimates provided in the RFI responses suggest that Phase 2 (Prototype Development) is likely to require the largest share of technical effort and financial resources. This observation confirms the importance of ensuring that the PCP phase structure and budget allocation provide sufficient flexibility and resources for integration, testing and iterative development.

Fifth, the responses revealed a strong interest in participating in the future PCP tender, with the majority of respondents indicating that they would likely participate and many expressing a preference for forming consortia with complementary partners. This confirms that the market is sufficiently active and diverse to support a competitive procurement process, while also suggesting that matchmaking and collaboration between specialised technology providers may play an important role in delivering integrated solutions.

Finally, several respondents provided recommendations related to governance, interoperability, operational validation and deployment conditions. These included requests for clearer information on pilot environments, existing infrastructure, interoperability constraints and operational validation scenarios. The SHIELD PCP consortium will take these considerations into account when finalising the PCP documentation and preparing the Call for Tender, with the objective of ensuring that the procurement framework remains realistic, competitive and conducive to innovation.

2. SHIELD PCP Scope

SHIELD PCP is a Horizon Europe funded project that brought together first responders, public authorities and technology providers to co-create innovative solutions for protecting public spaces and managing crowds in dynamic, high-risk environments. Building on the previous SHIELD4CROWD project, which identified common vulnerabilities and capability gaps, SHIELD PCP moved from analysis to joint innovation procurement by preparing a future PCP for integrated crowd protection solutions.

The project focused on a set of representative pilots capturing complex security challenges: panic at a football stadium in Slovakia, a drone attack on match day in Spain, and multi-actors' coordination after a massive knife attack in a French train station. Across these pilots, the Public Buyers Group (PBG) sought solutions that improved situational awareness, enabled multi-agency coordination, and supported informed decision-making and public communication, while respecting fundamental rights and data protection requirements.

The envisaged PCP is expected to procure R&D services that will lead to solutions reaching TRL 7-8, following the standard three-phase PCP model (solution design, prototype development, and validation and demonstration). The PBG, led by the French Ministry of Interior as Lead Procurer, will procure these services on behalf of the Ministries of Interior of France, Spain and Slovakia and SNCF, thereby ensuring a cross-border, multi-domain operational perspective. The OMC documented in this deliverable formed a key preparatory step to test the PCP concept with the market, reduce information asymmetries and ensure that the future tender is realistic, competitive and innovation-friendly.

3. Content deliverable

3.1. Open Market Consultation design and implementation

3.1.1. Objectives and methodology

The SHIELD PCP consortium designed the OMC to fulfil three main objectives:

- Validate the preliminary market and state-of-the-art analysis carried out under earlier work packages, including key technology trends and maturity levels relevant to the SHIELD PCP challenge.
- Inform and engage a broad community of potential suppliers, integrators and research organisations about the planned PCP, its scope, timetable and high-level requirements.

- Collect structured feedback on the feasibility of the proposed challenge, requirements and procurement approach, and identify potential risks, barriers and opportunities from a market perspective.

To achieve these objectives, the consortium combined qualitative and quantitative methods: online webinars in different EU languages; a hybrid event in Paris; and an RFI questionnaire administered through the EU Survey platform. The webinars and Paris event allowed for interactive presentations, live polling and open Q&A, while the RFI captured more detailed and comparable information across respondents.

All activities were conducted on a voluntary, non-binding basis, in line with Horizon Europe PCP rules and the OMC principles described in the SHIELD PCP OMC document. Participation in the OMC did not create any advantage or disadvantage in the future tender, and all contributions were anonymised in this report to protect legitimate business interests and ensure fair competition.

3.1.2. OMC timetable and participation

The OMC implementation followed the timetable announced in the OMC document, with minor adjustments in the final phase to reflect the actual publication and closure dates of the consortium. Table 1 below summarises the overall OMC timetable from the publication of the Prior Information Notice to the formal closure of the consultation.

Date	Event
24 November 2025	Publication of the Prior Information Notice (PIN) on TED.
18 December 2025	Publication of the OMC documents on the project's website: www.shieldpcp.eu Publication of the EU Survey questionnaire: https://ec.europa.eu/eusurvey/runner/SHIELD-PCP-RequestforInformation-Questionnaire
27 January 2026	OMC webinar in French
27 January 2026	OMC webinar in Spanish
28 January 2026	OMC webinar in Slovak
29 January 2026	OMC webinar in Polish
29 January 2026	OMC webinar in Italian
25-26 February 2026	OMC event in English – Paris, France (hybrid)
12 March 2026	Deadline for the submission of responses to the RFI questionnaire
20 March 2026	Publication of the OMC report
20 March 2026	Formal closure of the OMC

Table 1: OMC timetable of activities and required actions

Registration for all events was managed through the SHIELD PCP website (www.shieldpcp.eu), using an online form that collected basic information on participants and their organisations. The consortium monitored participation across

activities to ensure broad representation and identify gaps in stakeholder engagement.

Table 2 below summarises the number of **registered** and, where available, **actual** participants for each OMC activity, including the language-specific webinars, the hybrid Paris event and responses received to the RFI questionnaire via EU Survey.

Activity	Date(s)	Registered participants	Actual participants/responses
OMC webinar - French	27 January 2026	34	45
OMC webinar - Spanish	27 January 2026	88	82
OMC webinar - Slovak	28 January 2026	2	14
OMC webinar - Polish	29 January 2026	3	6
OMC webinar- Italian	29 January 2026	4	6
Hybrid OMC event - Paris	25-26 February 2026	131	54 technology providers (85 in total incl. consortium members and UOG members
RFI questionnaire (EU Survey)	Deadline 12 March 2026	49	49

Table 2: OMC participation per activity

The OMC document informed interested parties that the SHIELD PCP consortium reserved the right to adjust the planned activities and timetable. In practice, the OMC was implemented substantially as planned; the main adjustments concerned the finalisation phase, with the OMC report scheduled for publication on 19 March 2026 and the formal closure of the OMC on 20 March 2026, as reflected in Table 1.

3.2. OMC Webinars

3.2.1. Overview of webinars

Between 27 and 29 January 2026, the consortium organised five OMC webinars in different EU languages to reach a wide audience and facilitate participation from various countries. The webinars covered the same core content but were delivered in French, Spanish, Slovak, Polish and Italian, with slides and explanatory materials adapted as needed to the language and audience.

Each webinar lasted between 1 hour 28 minutes and 3 hours 15 minutes and followed the same structure. The French webinar (3 hours 15 minutes) was attended by 45 participants; the Spanish webinar (2 hours 11 minutes) by 82 participants; the Slovak webinar (1 hour 51 minutes) by 14 participants; the Polish webinar (1 hour 42 minutes) by 6 participants; and the Italian webinar (1 hour 28 minutes) by 6 participants. Each webinar consisted of four main parts: (i) introduction to SHIELD PCP and the PCP concept; (ii) presentation of the three pilots and the main functional and non-functional requirements; (iii) explanation of the OMC process, the RFI questionnaire

and the next steps; and (iv) interactive sessions, including live polls and Q&A. The webinars were recorded, in line with the privacy information included in the OMC document, and the recordings were used solely for internal analysis and quality assurance. The webinar recordings and presentation slides are made publicly available on the SHIELD PCP website: https://shieldpcp.eu/omc-webinars-recordings/.

3.2.2. Language-specific summaries

French webinar (27 January 2026)

The French webinar targeted technology providers, integrators and research organisations active in France and other French-speaking regions. It lasted approximately 3 hours and 15 minutes and was attended by 45 participants. The interactive session focused on collecting initial reactions to the three pilots and mapping potential contributions to the envisaged SHIELD PCP components, including analytics, sensing and command-and-control solutions.

Spanish webinar (27 January 2026)

The Spanish webinar lasted around 2 hours and 11 minutes and attracted 82 participants from Spain and other Spanish-speaking countries. The interactive session gathered inputs on how suppliers' solutions could address the pilot scenarios and highlighted particular interest in video analytics, drone-based sensing and integrated platforms.

Slovak webinar (28 January 2026)

The Slovak webinar lasted approximately 1 hour and 51 minutes and was attended by 14 participants. During the interactive segment, participants discussed how their solutions could be deployed in the "panic in a football stadium" pilot and raised questions on interoperability with existing national security systems.

Polish webinar (29 January 2026)

The Polish webinar, which lasted approximately 1 hour and 42 minutes, brought together 6 participants. The interactive session focused on potential contributions to detection and tracking components, as well as on integration with local command-and-control infrastructures.

Italian webinar (29 January 2026)

The Italian webinar lasted approximately 1 hour and 28 minutes and was attended by 6 participants. The interactive discussion explored possible Italian contributions to core SHIELD PCP components, with particular attention to AI-driven analytics and digital innovation solutions.

3.2.3. Polls and quantitative feedback

During the webinars, the consortium used Microsoft Teams polling functionality to collect instant feedback from participants on ten questions aligned with the RFI structure. For each question, participants selected predefined answer options, enabling a consolidated quantitative view across all language sessions (French, Spanish, Slovak, Polish and Italian). The detailed per-language results and the original Microsoft Teams screenshots are provided in Annex 1.

Q1. Have you already responded to the Request for Information (RFI) questionnaire?

Across all language sessions, only a small share of participants had already responded to the RFI at the time of the webinars. In the Spanish webinar, one respondent (5%) indicated "yes", while in the French webinar two respondents (22%) had already submitted the questionnaire. In the Slovak, Polish and Italian webinars, all respondents reported that they had not yet completed the RFI, confirming that the webinars played an important role in promoting the questionnaire and encouraging further responses.

Q2. In the stadium panic scenario shown, at which phase could your solution contribute the most?

The responses to Q2 indicate that suppliers see potential contributions across the full incident-management chain, with a concentration around early detection, situational awareness and evacuation support. In the larger Spanish and French webinars, multiple respondents selected early detection of suspicious behaviour or prohibited objects, real-time situational awareness and monitoring of crowd movement and evacuation, with additional interest in coordination between multiple agencies and communication with end users. The Slovak, Polish and Italian webinars, although involving fewer respondents, broadly mirrored this pattern, suggesting consistent interest in solutions that enhance awareness, coordination and crowd management throughout the stadium panic scenario.

Q3. For this pilot project, how would you position your contribution?

For Q3, most respondents positioned their organisations as providers of specific technology components or as integrators of multiple technologies into one solution. In the Spanish and French webinars, these two categories together accounted for the majority of responses, complemented by a substantial share of respondents offering analytical or decision-support capabilities and a smaller number focusing on operational implementation and validation. In the Slovak, Polish and Italian sessions, responses were more evenly distributed across the four main categories, but again tended to cluster around component provision and systems integration rather than participants who were still exploring how they could contribute.

Q4. In relation to this pilot scenario, your solution is best described as:

The answers to Q4 show that many solutions are at a relatively advanced stage of maturity, while still requiring some adaptation to the SHIELD PCP context. In the Spanish and French webinars, most respondents described their solutions as "applicable with adaptation or integration" or as "components that support part of the workflow", with a smaller group reporting solutions already used in comparable operational environments and, in the Spanish case, another group identifying solutions that are still under development or conceptual. In the Slovak, Polish and Italian sessions, respondents mainly indicated solutions that either require further development or represent core components that could be combined with other tools, highlighting the importance of integration and co-development during the PCP.

Q5. In the drone attack scenario shown, at which phase could your solution contribute the most?

Responses to Q5 confirm that participants' solutions can support multiple phases of a drone-related incident, with particular emphasis on detection, situational awareness and coordination. In the Spanish and French webinars, several respondents indicated

capabilities for early drone detection and classification, real-time situational awareness and multi-agency coordination, while others pointed to contributions to tracking, threat assessment and crowd-management functions. The Slovak, Polish and Italian sessions showed a similar distribution of interests, albeit with fewer respondents, again pointing to a broad range of technologies that can reinforce detection, monitoring and coordinated response in drone attack scenarios.

Q6. For this pilot project, how would you position your contribution?

The distribution of answers to Q6 suggests a balanced mix of technology components, platforms and supporting tools. In the Spanish webinar, responses were almost evenly split across core technology components, software platforms for coordination or situational awareness, decision-support or command-and-control tools and systems-integration solutions, with a smaller group focusing on crowd communication or evacuation support. The French webinar revealed a similar pattern, with core components, decision-support tools and integration solutions again strongly represented. In the Slovak, Polish and Italian sessions, respondents tended to select one or more of these same categories rather than concentrating on a single role, confirming that many suppliers see themselves contributing both specialised capabilities and integration or coordination functions.

Q7. In relation to this pilot scenario, your solution is best described as:

For Q7, most respondents characterised their solutions as requiring further development but fitting the pilot objectives, or as core components that could be combined with other solutions. In the Spanish and French webinars, these two categories together accounted for the majority of responses, with a smaller group indicating that their solutions were ready to be adapted and tested in real operational environments and very few considering their solutions not applicable to the pilot. In the Slovak, Polish and Italian sessions, the limited number of respondents was split between solutions requiring further development and core components suitable for combination with other tools, reinforcing the view that the PCP can leverage a mix of mature and near-to-market innovations.

Q8. In the knife attack scenario shown, at which phase could your solution contribute the most?

The responses to Q8 again point to strong capabilities in early detection, situational awareness and coordinated response. In the Spanish and French webinars, several participants selected early incident detection and initial alerts, rapid situational awareness and a common operational picture (COP) across agencies, with additional interest in multi-agency coordination and crowd-monitoring and evacuation-flow management; targeted communication to commuters and staff was less frequently selected. The Slovak, Polish and Italian sessions, though smaller, confirmed the same priorities, with respondents mainly indicating contributions to the common operational picture (COP) and coordination functions, complemented by some interest in crowd-monitoring and alerting.

Q9. For this pilot project, how would you position your contribution?

Answers to Q9 show that suppliers envisage their contributions both as central platforms and as specialised modules that can be combined into a broader system. In the Spanish and French webinars, respondents were distributed across central

platforms, specialised capabilities or modules and data-fusion or situational-awareness components, with a non-negligible share also indicating that support existing tools were less common. In the Slovak, Polish and Italian sessions, the few respondents generally positioned themselves as central platforms, data-fusion components or interoperability layers, confirming that many market actors see their added value in enabling coordination and integration across heterogeneous systems.

Q10. In relation to this pilot scenario, your solution is best described as:

Finally, Q10 highlights a clear predominance of software-based and AI-driven approaches, often in combination with hardware elements. Across the Spanish and French webinars, most respondents described their contributions as primarily software-based, as combined hardware-and-software solutions or as solutions based on data, analytics and artificial intelligence, with a smaller group indicating service- or operations-oriented offerings and almost no respondents identifying purely hardware-based solutions. The Slovak, Polish and Italian sessions followed a similar pattern, with respondents again favouring software-centric, data-driven and combined solutions and very few, if any, positioning themselves as hardware-only providers.

Overall, the polling results confirm strong market interest in solutions that enhance early detection, situational awareness, multi-agency coordination and interoperability, with a predominance of software-based, AI-driven and component-oriented contributions. These quantitative findings complement the qualitative feedback gathered during the webinars and the main OMC hybrid event, and were used by the consortium to refine the functional and non-functional requirements of the SHIELD PCP.

3.2.4. Webinar Q&A (all languages)

All webinars included a dedicated Q&A block that allowed participants to submit questions via the chat and orally, which the consortium answered live. Across the French, Spanish, Slovak, Polish and Italian sessions, a largely consistent set of questions emerged, focusing on eligibility and participation in the future PCP, consortium formation and matchmaking, the scope and maturity of expected solutions, intellectual property rights, data protection and ethical aspects, and the overall PCP budget and phase structure.

To ensure transparency and equal treatment in line with the principles of the TFEU, all questions raised during the webinars and the corresponding answers were consolidated into a written Q&A document. This document was published on the SHIELD PCP website (https://shieldpcp.eu/omc-webinars-recordings/) for all interested parties and is attached to this report as a separate file, Annex 2 – Consolidated Q&A (language-specific webinars), so that the information provided to suppliers ahead of the Call for Tender is fully documented and accessible in a single place.

3.3. OMC hybrid event in Paris

3.3.1. Agenda and format

The hybrid OMC event took place in Paris on 25 February 2026, bringing together representatives from the PBG, potential suppliers, research organisations and other stakeholders. The event combined plenary presentations, thematic sessions, and matchmaking opportunities, and was accessible both on site and online via streaming and interactive tools.

The agenda included:

- Opening session and project overview.
- Detailed presentations on the three SHIELD PCP pilots and the related operational contexts.
- Sessions on PCP rules, IPR, and evaluation criteria, helping suppliers understand the future tender.
- Short pitches and demonstrations by interested providers (15 pitches in total), covering:
  - AI-driven situational awareness and analytics,
  - Crowd monitoring and public space safety, including: density and flow analysis, behavioural monitoring and panic detection, evacuation management and safety optimisation,
  - Multi-sensor data fusion and interoperability, integration of video, acoustic, IoT, and wearable sensors, fusion of heterogeneous data streams into a Common Operational Picture (COP),
  - Decision support and command-and-control systems,
  - Drone and anti-drone technologies: detection and tracking of drones (including low-signature drones), anti-drone management systems, integration with broader security platforms,
  - Advanced sensing and hardware solutions: wearables and tracking devices for responders, acoustic sensors, magnetic sensing, and smart fabrics, and
  - Integrated platforms and system integration: large-scale platforms combining multiple technologies, system integration across agencies and domains.
- Facilitated matchmaking sessions to help suppliers identify potential partners and form consortia.

Hours	Topic	Presenter
	OMC event	
9:00 – 9:15	Registration	
9:15 – 9:30	Welcome & opening remarks	Etienne Genet *French Ministry of Interior*
9:30 – 10:00	Explanation of the SHIELD PCP project (rationale, use cases, PCP process)	Nina Czyżewska *Polish Platform for Homeland Security*
10:00 – 10:45	Presentation of the state-of-the-art analysis	Youssef Bouali *DIGINNOV*
10:45 – 11:00	Coffee break	
11:00 – 11:20	OMC objectives and activities	Azra Atalan *CORVERS*
11:20 – 12:20	Interactive session	Moderator: Youssef Bouali, *DIGINNOV* All participants
12:20 – 13:00	Next steps	Nina Czyżewska *Polish Platform for Homeland Security*
13:00 – 14:00	*Lunch break*	
	Matchmaking session	
14:00 – 14:10	Introduction to the matchmaking session	Nina Czyżewska *Polish Platform for Homeland Security*
14:10 – 15:10	Presentation by suppliers of their company and capabilities	All participants
15:10 – 16:00	Matchmaking session	All participants
16:00 – 16:10	Closure	Nina Czyżewska *Polish Platform for Homeland Security*

Table 3: OMC hybrid Paris event - agenda

3.3.2. Participation and stakeholder profile

Participation in the Paris event was open to all interested parties, with priority for on-site places given to organisations that had submitted or planned to submit an RFI questionnaire. In total, 131 technology providers registered for the event.

The event attracted a broad spectrum of stakeholders, including providers of AI-based analytics, sensor systems, communication and networking technologies, command-and-control platforms, and integration services. Actual participation comprised 54 technology providers (85 participants in total when including consortium members and members of the User Observatory Group (UOG)), with a strong presence of SMEs alongside several larger industry players and research organisations, as well as a number of new entrants to the SHIELD PCP topic.

3.3.3. Main discussion points and feedback

Discussions in Paris focused on several key themes:

- Technical feasibility of the SHIELD PCP requirements and potential integration architectures for multi-agency platforms.
- Challenges related to deploying solutions in real operational environments such as stadiums, train stations and urban public spaces.
- Legal and ethical aspects, including GDPR compliance, proportionality of surveillance technologies and transparency towards citizens.

- Business models for long-term sustainability beyond the PCP, including maintenance, updates and cross-border deployment.

Participants generally welcomed the PCP approach and the cross-border nature of the PBG, which they viewed as an opportunity to scale innovative solutions beyond national markets. At the same time, suppliers highlighted the importance of clear and realistic requirements, phased testing and adequate support for interoperability and integration.

During the Paris hybrid event on 25 February 2026, the consortium used live polling via Mentimeter to collect structured, anonymous feedback from participants on their current capabilities and plans in relation to the SHIELD PCP requirements. While the earlier language-specific webinars focused primarily on pilot-oriented questions exploring potential technological contributions within the three presented scenarios, the interactive session during the Paris event adopted a more solution-oriented perspective. In the period leading up to the event, the project requirements and technical framework had been further refined based on internal project work and preliminary feedback received from the market. Consequently, the Mentimeter polling focused on key functional components of the envisaged SHIELD PCP solution, including aspects such as system integration, data fusion, interoperability, operational workflows and indicative cost considerations. The results indicated that only a small subset of suppliers currently operate mature, large-scale solutions in complex stadium and urban environments, with many positioning their capabilities at prototype or pilot stage. Advanced functionalities such as dynamic evacuation optimisation, real-time multi-layer data fusion and federated multi-agency integration were generally less mature, whereas there was strong but heterogeneous interest and activity in AI-driven crowd analytics, drone and anti-drone technologies, secure and resilient communications, and non-biometric movement and behaviour monitoring compliant with EU legal and data-protection requirements. This approach allowed the consortium to validate with market participants its updated understanding of the project's technical requirements and market readiness. The detailed results of the Mentimeter polling conducted during the Paris OMC event are provided in Annex 3.

3.4. Request for Information (RFI) questionnaire

3.4.1. Structure of the questionnaire

The RFI questionnaire, made available via the EU Survey platform and annexed to the OMC document, invited technology providers and other stakeholders to provide written input on their solutions, capabilities and views in relation to the SHIELD PCP challenge. The questionnaire consisted of 37 questions (Q1-Q37) covering the following aspects:

- General information about the organisation (type, size, country, contact details).
- Description of relevant solutions or technologies and the SHIELD PCP pilots they addressed.
- Assessment of technology readiness (TRL), roadmap and expected developments.

- Questions on legal, ethical and societal aspects, including data protection and fundamental rights.
- Views on interoperability, standards and integration with existing systems.
- Expectations regarding PCP phases, timelines and budget.
- Interest in participating in the future PCP and preferred forms of collaboration (single entity or consortium).

Participation in the RFI was voluntary and non-binding, and respondents were advised not to include confidential or proprietary information. All responses were later anonymised for the purposes of this report.

3.4.2. Response rate and respondent profile

By the deadline of 12 March 2026, 49 valid responses to the RFI questionnaire had been received. Respondents represented 6 countries, with the largest shares coming from Spain (23 responses) and France (18 responses), followed by Italy (3 responses), Greece (2 responses), Belgium (1 response) and Slovakia (2 responses).

In terms of organisation type, the responses show a strong predominance of market actors from the SME and start-up ecosystem, alongside a significant presence of larger companies and a smaller number of research organisations/universities and other private entities. Based on the EU Survey statistics, respondents selected the following organisation categories: SME (24 selections), large company (13), start-up (11), R&D institute/university (3), private organisation (2) and other (1), while no respondent selected public organisation. As some respondents selected more than one category, these figures should be read as declared profiles rather than mutually exclusive classes. Overall, the respondent base was composed mainly of solution providers, technology developers and systems integrators active in areas such as crowd analytics, command-and-control platforms, sensor integration, secure communications, counter-drone technologies, geolocation, CBRN-related capabilities and crisis-management software.

Type of organisation:

		Answers	Ratio
Start-up		11	22.45 %
SME		24	48.98 %
Large company		13	26.53 %
Public organisation		0	0 %
Private organisation		2	4.08 %
R&D institute / University		3	6.12 %
Other		1	2.04 %
No Answer		0	0 %

Figure 1: Type of Organisations

3.4.3. Main findings per questionnaire section

Q1. Are you aware of any existing or emerging technologies in the field of protection of public spaces and crowd management (as described in SHIELD PCP)?

Out of 49 respondents, 41 indicated that they were aware of existing or emerging technologies in this field, while 8 answered negatively. The answers show a broad and

active technology landscape, with respondents referring in particular to AI-enabled video and image analytics, crowd-behaviour monitoring, LiDAR and other non-biometric sensing approaches, multi-sensor fusion, secure and resilient communications, drone and counter-drone capabilities, geolocation and tracking solutions, CBRN-related sensing, and data-sharing or data-space approaches for multi-agency coordination. Several responses also indicated that the market is increasingly moving towards integrated platforms that combine sensing, analytics, alerting and operational decision-support rather than standalone tools.

		Answers	Ratio
Yes		41	83.67 %
No		8	16.33 %
No Answer		0	0 %

Figure 2: Awareness of the existing technologies

Q2. Are you currently developing or have you developed any solution relevant to any of the following use cases? (Tick all that apply and describe briefly)

- ☐ Use Case 1: Panic at football stadium.
- ☐ Use Case 2: Drone Attack Match Day.
- ☐ Use Case 3: Multi-actors coordination after a massive knife attack in a train station.
- ☐ No solution was developed for any of the use cases above.

The answers confirm that the great majority of respondents are active in at least one SHIELD PCP scenario. Use Case 1 (panic at a football stadium) was selected by 41 respondents, Use Case 2 (drone attack on match day) by 36 respondents, and Use Case 3 (multi-actor coordination after a massive knife attack in a train station) by 30 respondents, while only 5 indicated that they had not developed a relevant solution for any of the listed use cases. The described solutions cover a wide spectrum, including crowd monitoring and anomaly detection, geolocation and movement tracking, command-and-control platforms, multi-source fusion environments, drone and counter-drone technologies, secure communications, situational-awareness tools, simulation and training environments, and specialised sensing capabilities. Many respondents stressed that their technologies are inherently multi-use-case and can be adapted across stadiums, transport hubs and other public-space environments.

		Answers	Ratio
Use Case 1: Panic at football stadium.		41	83.67 %
Use Case 2: Drone Attack Match Day.		36	73.47 %
Use Case 3: Multi-actors coordination after a massive knife attack in a train station.		30	61.22 %
No solution was developed for any of the use cases above.		5	10.2 %
No Answer		0	0 %

Figure 3: Solutions relevant to the pilots

Q3. Which of the following capability areas do you consider most critical to address these scenarios? (Select up to 3 options)

- ☐ Real-time common operational picture (COP) and dashboards for commanders
- ☐ Crowd behaviour monitoring and analytics (e.g. detecting surges, panic)
- ☐ Counter-drone detection and neutralisation systems
- ☐ AI-supported decision-making tools for incident management
- ☐ Inter-agency communication and coordination platform
- ☐ Multi-source data fusion and sensor integration
- ☐ Evacuation support and crowd routing systems
- ☐ Public alerting and communication to citizens (e.g. emergency messaging)

Respondents prioritised integrated operational awareness and data fusion very clearly. The most frequently selected capability areas were real-time common operational picture and commander dashboards (33 selections), multi-source data fusion and sensor integration (30), and crowd-behaviour monitoring and analytics (28). These were followed by AI-supported decision-making tools (20), counter-drone detection and neutralisation (17), and inter-agency communication and coordination platforms (15). Evacuation support and crowd routing (12) and public alerting to citizens (10) were selected less often, although they still emerged as relevant. Overall, the answers show that suppliers see the main challenge not as a single isolated function but as the combination of awareness, analytics, fusion and operational coordination.

		Answers	Ratio
Real-time common operational picture (COP) and dashboards for commanders		33	67.35 %
Crowd behaviour monitoring and analytics (e.g. detecting surges, panic)		28	57.14 %
Counter-drone detection and neutralisation systems		17	34.69 %
AI-supported decision-making tools for incident management		20	40.82 %
Inter-agency communication and coordination platform		15	30.61 %
Multi-source data fusion and sensor integration		30	61.22 %
Evacuation support and crowd routing systems		12	24.49 %
Public alerting and communication to citizens (e.g. emergency messaging)		10	20.41 %
No Answer		0	0 %

Figure 4: Critical areas to address

Q4. What are the safety mechanisms and fail-safe features your solution would include to avoid collateral damage or unintended consequences?

Across the responses, a strong pattern emerges around human control, conservative system behaviour and accountability. Respondents frequently stated that critical operational decisions should remain human-led, with technology supporting but not replacing operators. Many answers referred to fail-safe or fallback modes, graceful degradation in case of component failure, redundancy, cross-validation of detections, configurable thresholds to reduce false positives, and clear escalation logic. Privacy- and security-by-design were also recurring themes, including

encryption, access control, logging, auditability, data minimisation, anonymisation and use of less intrusive sensing modalities where possible. Some respondents additionally described domain-specific precautions, such as passive monitoring modes, safe landing or retraction features for aerial systems, and tight restrictions around any active countermeasure functions.

Q5. Do you identify any technical, operational or organisational barriers, gaps or missing needs in relation to the scope and requirements of SHIELD PCP?

A substantial share of the market identified barriers or gaps: 24 respondents answered yes, 22 answered no, and 3 provided no answer. The issues raised most often concerned interoperability across heterogeneous and legacy systems, data-sharing constraints between organisations, multi-agency coordination in time-critical situations, legal uncertainty for some security technologies, and the operational challenge of turning large volumes of sensor and AI outputs into reliable and trusted decision support. Respondents also pointed to gaps around cross-border governance, semantic interoperability, communications resilience, privacy-compliant analytics, high-precision tracking in complex environments, and the organisational readiness of end users to deploy emerging technologies at scale.

		Answers	Ratio
Yes		24	48.98 %
No		22	44.9 %
No Answer		3	6.12 %

Figure 5: Technical, operational or organisational gaps/barriers

Q6. Can your solution be modularised or integrated with external platforms or APIs (e.g., EMS, law enforcement systems)?

The market response was very strong on this point: 46 respondents answered yes and none answered no, while 3 left the question blank. The explanations show that modularity and integration-readiness are now standard expectations among suppliers. Many respondents described API-first or modular architectures, support for common protocols, use of adapters or middleware for legacy environments, and the ability to connect with EMS, C2, VMS, CCTV, GIS, public-safety communications and other external platforms. The answers indicate that the future PCP can realistically expect interoperable building blocks rather than purely closed, standalone systems.

		Answers	Ratio
Yes		46	93.88 %
No		0	0 %
No Answer		3	6.12 %

Figure 6: The modularity of solutions

Q7. If you were to participate in the SHIELD PCP, please indicate your indicative time allocation (in months) for each of the following phases: *(Total should not exceed 23 months)*

	Number of months
*Phase 1: Solution Design:	
*Phase 2: Prototype Development:	
*Phase 3: Validation & Demonstration:	

Respondents generally envisaged a PCP time profile in which Phase 1 is relatively short, Phase 2 is the longest and most technically demanding, and Phase 3 requires sufficient time for validation in operational conditions. Across the submitted estimates, Phase 1 was most often placed in the 3 to 6 month range, Phase 2 typically in the 8 to 12 month range, and Phase 3 most often in the 4 to 8 month range, although some respondents proposed longer validation periods depending on pilot complexity. The justifications show that suppliers expect the main effort to lie in system engineering, integration, adaptation of analytics, prototype development, and iterative testing before final demonstration in real environments.

Q8. If you were to participate in the SHIELD PCP, please provide your indicative budget allocation (in EUR) per PCP phase: *(Please be aware that there is a predefined budget allocation for this PCP project, and the total available budget will be divided across phases and participating contractors. For the purpose of this question, please assume a total indicative PCP budget of EUR 3,600,000.)*

	Amount of budget
*Phase 1: Solution Design (€):	
*Phase 2: Prototype Development (€):	
*Phase 3: Validation & Demonstration (€):	

The budget estimates varied considerably, confirming that respondents made different assumptions about consortium size, hardware intensity, maturity of existing assets and scale of piloting. Nevertheless, the qualitative pattern was consistent: most respondents allocated the largest budget share to Phase 2, which they associated with integration work, software and analytics development, hardware procurement, testing and optimisation. Phase 1 was generally budgeted lower, mainly for design, architecture, requirements refinement, planning and governance work. Phase 3 budgets were more variable, with some respondents expecting limited validation costs and others anticipating substantial expenditure for field trials, deployment, travel, calibration, training and stakeholder engagement. Overall, the responses support the view that prototype development is expected to be the main cost concentration point in the PCP.

Q9. Do you feel that the use cases and requirements described (spanning common operational picture, crowd monitoring, geolocation tracking, communications, etc.) cover all the critical needs of the PCP challenge? Are there many significant challenges or needs that you believe are missing from our list?

Most respondents considered that the use cases and requirements provide a good overall baseline for the PCP challenge. At the same time, a notable number of answers

suggested that some aspects should be strengthened or made more explicit. The most frequently mentioned additions or refinements concerned CBRN-related needs, planning and preparedness functions, simulation and training, persistent aerial or wide-area awareness, faster automated alerting to responders, stronger treatment of privacy and cryptographic resilience, clearer governance and data-sharing rules, and more detailed prioritisation of requirements to avoid excessive breadth. The feedback therefore supports the current direction of the PCP, while suggesting that requirement framing should remain focused, operational and legally robust.

Q10. Which of the listed requirements in Annex III do you anticipate being the most technically or operationally challenging to implement, and what makes them challenging? Please highlight any requirements you see as high-risk or particularly complex.

Respondents consistently identified integrated, real-time and cross-organisational functions as the most challenging. The answers most often referred to multi-source data fusion, interoperability with legacy systems, advanced AI-based analytics, trusted decision support, resilient communications, and fine-grained access control across multiple agencies. Many respondents underlined the challenge of maintaining low latency and high reliability while also ensuring explainability, GDPR compliance, secure data handling, and operational usability in stressful environments. Additional complexities mentioned include indoor or dense-environment localisation, counter-drone functions, evacuation optimisation, behavioural analytics, and large-scale validation in realistic pilot conditions.

Q11. What do you anticipate will be the main cost drivers in developing and deploying an integrated solution for these scenarios? *(Select up to 2 options.)*

- ☐ Specialised hardware (e.g. sensors, drones, cameras)
- ☐ Software development (analytics, AI algorithms, user interfaces)
- ☐ System integration of components and data sources
- ☐ Communication infrastructure (networks, devices, radios)
- ☐ Training and change management for end-users
- ☐ Ongoing maintenance and support of the system.
- ☐ Other

Software development was the most frequently selected cost driver (34 selections), followed by system integration of components and data sources (27) and specialised hardware such as sensors, drones and cameras (23). Communication infrastructure was selected 10 times, while training and change management (5), ongoing maintenance and support (3), and other costs (2) were mentioned less frequently. The overall picture is that respondents see cost pressure arising above all from the complexity of building and integrating a usable multi-component solution, not only from buying equipment.

		Answers	Ratio
Specialised hardware (e.g. sensors, drones, cameras)		23	46.94 %
Software development (analytics, AI algorithms, user interfaces)		34	69.39 %
System integration of components and data sources		27	55.1 %
Communication infrastructure (networks, devices, radios)		10	20.41 %
Training and change management for end-users		5	10.2 %
Ongoing maintenance and support of the system.		3	6.12 %
Other		2	4.08 %
No Answer		0	0 %

Figure 7: The main cost drivers

Q12. Which approach do you believe is more effective for delivering the solution sought in this PCP? *(Select one option.)*

- ○ A single-vendor integrated platform (one provider/consortium delivering all components as a unified system)
- ○ A modular solution (multiple specialised components from different providers, designed to interoperate)
- ○ No strong preference / Either approach can work

A clear majority of respondents favoured a modular approach: 34 selected a modular interoperable solution, 9 expressed no strong preference, and only 6 preferred a single-vendor integrated platform. The comments and related answers throughout the questionnaire reinforce this result. Respondents broadly see the SHIELD PCP challenge as best addressed by combining specialised components through open interfaces and strong integration, rather than by expecting one monolithic system to cover the full functional scope.

		Answers	Ratio
A single-vendor integrated platform (one provider /consortium delivering all components as a unified system)		6	12.24 %
A modular solution (multiple specialised components from different providers, designed to interoperate)		34	69.39 %
No strong preference / Either approach can work		9	18.37 %
No Answer		0	0 %

Figure 8: The allocation of the answers

Q13. How important is it that the solution uses open standards and interfaces to interoperate with existing systems and third-party components? *Move the slider or accept the initial position.*

Move the slider or accept the initial position.

Not important — Very important

0

0 — 5

The importance attached to open standards and interfaces was very high. Among the non-blank answers, 28 respondents selected the highest score and 11 selected the second-highest score, while only 2 respondents gave very low scores. This shows a strong market expectation that SHIELD PCP solutions should interoperate with existing systems and future third-party components through open or widely adopted interfaces, thereby reducing lock-in and facilitating long-term scalability.

		Answers	Ratio
0		1	2.04 %
1		1	2.04 %
2		0	0 %
3		5	10.2 %
4		11	22.45 %
5		28	57.14 %
No Answer		3	6.12 %

Figure 9: The importance of open standards and interfaces

Q14. Can you provide any other recommendations regarding the SHIELD PCP solution(s)?

Twenty-one respondents provided additional recommendations, 23 answered no, and 5 gave no answer. The additional suggestions were broadly aligned with the rest of the questionnaire: stronger legal and ethical compliance by design, especially for AI and personal-data processing; careful specification of interoperability requirements; practical deployability in real operational environments; early and sustained involvement of end users; and support for preparedness, simulation, training and resilient communications. Some respondents also recommended broadening sensing options and ensuring that the future tender remains sufficiently open to innovative combinations of components.

State-of-the-art analysis

Q15. Do you think there is room for technological development beyond the state of the art?

Yes was the dominant answer: 40 respondents said yes, 5 said no and 4 gave no answer. The explanations indicate that respondents see substantial room for innovation beyond today's market offerings, particularly in privacy-preserving crowd analytics, real-time multi-sensor fusion, edge processing, predictive modelling, AI-supported decision support, scalable interoperability and more operationally mature deployment models. A recurring point was that while many individual building blocks already exist, the SHIELD PCP challenge lies in improving their maturity, integration and field-readiness in a demanding public-safety context.

		Answers	Ratio
Yes		40	81.63 %
No		5	10.2 %
No Answer		4	8.16 %

Figure 10: The allocation of the answers

Funded by the European Union

Q16. What is the current Technology Readiness Level (TRL) of your solution(s) or their main components? *Please indicate the TRL for the relevant functional requirement groups described in the OMC document (Annex III), if applicable.*

The TRL information provided by respondents shows a mixed market maturity profile. Most answers place the relevant solutions or main components broadly in the TRL 5 to 8 range, with some mature building blocks already at TRL 8 or 9 and a smaller number of innovative or SHIELD-specific modules still at earlier stages, typically around TRL 2 to 4. Several respondents clearly distinguished between mature core components and less mature extensions needed for the specific SHIELD PCP challenge. This suggests that the market is sufficiently mature for PCP, but that additional R&D is still needed to move from component-level readiness to integrated operational solutions.

Q17. What are the main limitations of the current state of the art that your solution aims to address, and what improvements would it introduce compared to existing approaches would your solution introduce?

Respondents described current market limitations in terms of fragmentation, lack of integration, insufficient predictive capability, overreliance on conventional camera-based monitoring, operational latency, weak interoperability and limited legal or organisational readiness for advanced analytics. Many answers stressed that current systems are still too reactive, too siloed, or too dependent on manual interpretation by operators. The improvements proposed by respondents therefore focused on richer sensing, better fusion of heterogeneous data, stronger decision-support functions, privacy-preserving analytics, improved tracking and geolocation, more resilient communications, and faster operational workflows that support anticipation rather than only post-event reaction.

Q18. Do you rely on any patented technology or standards?

19 respondents answered yes, 25 answered no and 5 did not provide an answer. Those answering yes generally referred to proprietary technologies combined with recognised technical or operational standards. The answers indicate that some respondents bring protected know-how or patented elements into the field, but the market also includes many suppliers relying primarily on non-patented in-house developments, standard protocols and generally available methods. This mix suggests that IPR exists in the market, but not in a way that appears to block participation or prevent modular solution-building.

		Answers	Ratio
Yes		19	38.78 %
No		25	51.02 %
No Answer		5	10.2 %

Figure 11: The allocation of the answers

Q19. Are there existing patents or intellectual property barriers that could limit your solution's development or deployment?

The answers were overwhelmingly negative: 44 respondents answered no, 1 answered yes, and 4 gave no answer. The single positive answer was cautious and non-specific.

Overall, the market does not currently appear to perceive third-party patents or IP barriers as a major obstacle to development or deployment in the SHIELD PCP context, although this will still need to be managed carefully at tender and consortium level.

Q20. Which of the following areas already have mature solutions available on the market (high readiness, e.g. TRL 8-9)? *(Select all that apply.)*

- ☐ Real-time common operational picture (COP) and dashboards for commanders
- ☐ Crowd behaviour monitoring and analytics (e.g. detecting surges, panic)
- ☐ Counter-drone detection and neutralisation systems
- ☐ AI-supported decision-making tools for incident management
- ☐ Inter-agency communication and coordination platform
- ☐ Multi-source data fusion and sensor integration
- ☐ Evacuation support and crowd routing systems
- ☐ Public alerting and communication to citizens (e.g. emergency messaging)
- ☐ I do not know.

Respondents most frequently saw mature market solutions in public alerting and communication to citizens (30 selections) and real-time common operational picture/dashboards (28). These were followed by inter-agency communication and coordination platforms (19), multi-source data fusion and sensor integration (17), and counter-drone detection and neutralisation (15). Fewer respondents considered crowd-behaviour monitoring (10), evacuation support (9) and especially AI-supported decision-making (8) to be fully mature. Ten respondents also selected "I do not know", which indicates that market maturity is still uneven and sometimes difficult to assess consistently across all capability areas.

		Answers	Ratio
Real-time common operational picture (COP) and dashboards for commanders		28	57.14 %
Crowd behaviour monitoring and analytics (e.g. detecting surges, panic)		10	20.41 %
Counter-drone detection and neutralisation systems		15	30.61 %
AI-supported decision-making tools for incident management		8	16.33 %
Inter-agency communication and coordination platform		19	38.78 %
Multi-source data fusion and sensor integration		17	34.69 %
Evacuation support and crowd routing systems		9	18.37 %
Public alerting and communication to citizens (e.g. emergency messaging)		30	61.22 %
I do not know.		10	20.41 %
No Answer		0	0 %

Figure 12: The maturity of the solutions (TRL 8-9)

Q21. In which areas do you see the least mature state-of-the-art, requiring the most innovation? *(Select up to 3 options that represent the biggest gaps.)*

- ☐ Real-time common operational picture (COP) and dashboards for commanders
- ☐ Crowd behaviour monitoring and analytics (e.g. detecting surges, panic)
- ☐ Counter-drone detection and neutralisation systems
- ☐ AI-supported decision-making tools for incident management
- ☐ Inter-agency communication and coordination platform
- ☐ Multi-source data fusion and sensor integration
- ☐ Evacuation support and crowd routing systems
- ☐ Public alerting and communication to citizens (e.g. emergency messaging)
- ☐ I do not know.

The biggest perceived innovation gaps were crowd-behaviour monitoring and analytics (28 selections) and AI-supported decision-making tools for incident management (24). These were followed by counter-drone detection and neutralisation (16), multi-source data fusion and sensor integration (15), evacuation support and crowd routing (12), and inter-agency communication and coordination (10). Very few respondents saw the common operational picture itself as a major maturity gap. Overall, respondents appear to consider that visualisation layers are relatively mature, whereas high-quality analytics, trustworthy AI support and deeper operational automation still require significant innovation.

		Answers	Ratio
Real-time common operational picture (COP) and dashboards for commanders		3	6.12 %
Crowd behaviour monitoring and analytics (e.g. detecting surges, panic)		28	57.14 %
Counter-drone detection and neutralisation systems		16	32.65 %
AI-supported decision-making tools for incident management		24	48.98 %
Inter-agency communication and coordination platform		10	20.41 %
Multi-source data fusion and sensor integration		15	30.61 %
Evacuation support and crowd routing systems		12	24.49 %
Public alerting and communication to citizens (e.g. emergency messaging)		5	10.2 %
I do not know.		6	12.24 %
No Answer		0	0 %

Figure 13: The least mature state-of-the-art

Q22. Which emerging technologies do you think could significantly enhance solutions for these scenarios? *(Select up to 3 options.)*

- ☐ Artificial Intelligence / Machine Learning
- ☐ Internet of Things (IoT) sensors and smart cameras
- ☐ 5G or advanced wireless communication networks
- ☐ Cloud computing and edge processing for real-time data
- ☐ Advanced drone technologies and robotics
- ☐ Big data analytics and predictive modelling
- ☐ Other

Artificial intelligence and machine learning clearly dominated this question, with 42 selections. Cloud and edge processing (24), IoT sensors and smart cameras (23), and big-data analytics and predictive modelling (20) were also highly visible, followed by advanced drone technologies and robotics (16) and 5G or advanced wireless communications (12). The smaller number of "other" answers pointed to additional enabling technologies such as advanced security layers, digital-twin or immersive environments, and highly deployable modular architectures. Taken together, the results show that respondents view the future SHIELD PCP solution space as strongly data-driven, analytics-enabled and integration-focused.

		Answers	Ratio
Artificial Intelligence / Machine Learning		42	85.71 %
Internet of Things (IoT) sensors and smart cameras		23	46.94 %
5G or advanced wireless communication networks		12	24.49 %
Cloud computing and edge processing for real-time data		24	48.98 %
Advanced drone technologies and robotics		16	32.65 %
Big data analytics and predictive modelling		20	40.82 %
Other		4	8.16 %
No Answer		0	0 %

Figure 14: The allocation of the answers

Miscellaneous

Q23. What additional information, requirements of clarifications (if any) would you need to make a well-founded plan for the development and/or deployment of a solution within SHIELD PCP?

A substantial part of the market requested more detailed planning information. Respondents most often asked for clearer information on pilot sites, layouts and existing infrastructure; more detailed and prioritised functional and operational requirements; clearer interoperability and API conditions; data-governance and security constraints; performance expectations such as latency, bandwidth and availability; and clearer validation criteria for pilots. Several answers also indicated a need for better understanding of the organisational context, access rules, and consortium-building opportunities. This shows that suppliers are interested, but many need more operational detail before they can build robust implementation plans.

Q24. Would your organisation consider participating in the upcoming SHIELD PCP procurement (tender) as a solution provider? *(Select one.)*

- ○ Yes – we would likely participate
- ○ Maybe – we need more information/depends on conditions
- ○ No – unlikely to participate

Market interest in the future tender was very strong. 41 respondents answered that they would likely participate, 8 selected maybe/depending on conditions, and none selected unlikely to participate. This is an important signal that the OMC succeeded in mobilising the market and that the forthcoming procurement should attract substantial competition, provided the tender remains realistic and clearly specified.

		Answers	Ratio
Yes – we would likely participate		41	83.67 %
Maybe – we need more information/depends on conditions		8	16.33 %
No – unlikely to participate		0	0 %
No Answer		0	0 %

Figure 15: Willingness to participate

Q25. Do you intend to participate as a single entity or as part of a consortium?

- ○ Single entity
- ○ Consortium

The majority of respondents envisage participating through consortia rather than alone. Thirty-eight selected consortium participation, while 11 selected single entity. The accompanying explanations show that many respondents are actively looking for complementary partners, especially in integration, communications, sensing, counter-drone, crowd analytics, public alerting, command-and-control and other specialised modules. This strongly supports a PCP design that allows and encourages collaborative, multi-actor solution teams.

Q26. Could you please indicate the name of your proposed solution or innovation?

Most respondents provided either a working name or at least a short identifier for their proposed solution, while a smaller group indicated that the name was still to be defined. As confidential naming should not be reproduced in the public report, the answers can be grouped into broad families: integrated crowd-monitoring and decision-support platforms; spatial intelligence and tracking solutions; drone and counter-drone systems; secure communications and crisis-management tools; CBRN-related sensing and response capabilities; and other specialised public-safety technologies. The answers confirm a diverse market with both broad platforms and niche technical modules.

Q27. Could you please provide an image or visual representation of your proposed solution or innovation, if available?

Around half of the respondents provided at least one visual, image file or other visual reference, while the remainder did not. Where provided, the visuals generally appeared to serve as illustrative support for solution concepts, system architectures or key components rather than as detailed technical documentation. For the report, it is sufficient to note that a meaningful share of respondents was able to support its submission with visual material, but that such material should remain outside the anonymised analytical summary unless explicitly cleared for publication.

Funded by the European Union

Q28. Which modules or macro-functionalities does your proposed solution intend to address?

- ☐ Real-time common operational picture (COP) and dashboards for commanders
- ☐ Crowd behaviour monitoring and analytics (e.g. detecting surges, panic)
- ☐ Counter-drone detection and neutralisation systems
- ☐ AI-supported decision-making tools for incident management
- ☐ Inter-agency communication and coordination platform
- ☐ Multi-source data fusion and sensor integration
- ☐ Evacuation support and crowd routing systems
- ☐ Public alerting and communication to citizens (e.g. emergency messaging)
- ☐ None

The strongest concentration of proposed solution coverage was around common operational picture and dashboards (36 selections), multi-source data fusion and sensor integration (35), crowd-behaviour monitoring and analytics (34), and AI-supported decision-making tools (31). Inter-agency communication and coordination also featured strongly (24), while counter-drone functions (18), evacuation support (14) and public alerting (10) were less frequently selected. Only one respondent selected none. The responses show that the market is particularly concentrated around platform, fusion and analytics capabilities, with fewer actors focusing primarily on citizen communication or evacuation management.

		Answers	Ratio
Real-time common operational picture (COP) and dashboards for commanders		36	73.47 %
Crowd behaviour monitoring and analytics (e.g. detecting surges, panic)		34	69.39 %
Counter-drone detection and neutralisation systems		18	36.73 %
AI-supported decision-making tools for incident management		31	63.27 %
Inter-agency communication and coordination platform		24	48.98 %
Multi-source data fusion and sensor integration		35	71.43 %
Evacuation support and crowd routing systems		14	28.57 %
Public alerting and communication to citizens (e.g. emergency messaging)		10	20.41 %
None		1	2.04 %
No Answer		0	0 %

Figure 16: The macro-functionalities which were intended to address

Q29. How would you describe your technology, and how does it relate to the SHIELD PCP requirements?

Respondents commonly described technologies that map directly onto the SHIELD PCP requirement structure, especially in relation to real-time situational awareness, crowd monitoring, AI analytics, sensor fusion, secure communications, command support and interoperability with existing systems. Some respondents positioned themselves as broad solution providers spanning several requirement groups, while

others clearly targeted a subset of the PCP scope, such as tracking, drone-related functions, specialised sensing, or communications resilience. Overall, the answers confirm that the market contains both integrative platforms and specialised modules that could contribute to a modular SHIELD PCP ecosystem.

Q30. How would you describe the innovation level of your technology and its differentiation from the current state of the art? *(Please describe the innovation aspects of your solution, the state of the art in the market, and how your solution is differentiated.)*

The responses consistently framed innovation in terms of better integration, stronger real-time awareness, more advanced analytics, privacy-preserving or edge-based processing, improved operational usability, and better adaptation to public-safety contexts. Many respondents argued that their differentiation lies not necessarily in inventing an entirely new single technology, but in combining technologies more effectively, reducing operator burden, improving prediction and early warning, and making solutions more deployable, more explainable and more interoperable than current alternatives. This supports the idea that SHIELD PCP should value system-level innovation and operational impact, not only novelty of isolated components.

Q31. What is the target market addressed, and who will use your technology? (Please indicate which user groups your solution addresses.)

- ☐ Public bodies (e.g., law enforcement agencies, civil protection authorities, cities, defence sector)
- ☐ Private-sector security operators (e.g., guarding services, event security management)
- ☐ Mixed public-private security operators (e.g., critical infrastructure operators, utilities)

The target-user profile is clearly centred on public and mixed security environments. Mixed public-private security operators were selected by 40 respondents and public bodies by 39, while 27 also selected private-sector security operators. The additional descriptions indicate that intended users include law-enforcement and civil-protection actors, transport and critical-infrastructure operators, venue or event-security organisations, and other entities responsible for safety and incident response in crowded or sensitive environments. The answers therefore confirm that the proposed technologies are highly relevant to the operational setting envisaged by SHIELD PCP.

		Answers	Ratio
Public bodies (e.g., law enforcement agencies, civil protection authorities, cities, defence sector)		39	79.59 %
Private-sector security operators (e.g., guarding services, event security management)		27	55.1 %
Mixed public-private security operators (e.g., critical infrastructure operators, utilities)		40	81.63 %
No Answer		0	0 %

Figure 17: The allocation of the answers

Q32. What are the main technological, legal, ethical or operational risks and challenges associated with the development and deployment of your solution, and how could these be mitigated? Please explain.

Many respondents highlighted data protection, privacy and AI-governance considerations as key risks, particularly when processing video or other sensitive data

in public spaces. Suggested mitigation measures include privacy-by-design approaches, strong encryption, access control mechanisms and human-in-the-loop decision making.

Several answers also pointed to technical and operational challenges, including integration with heterogeneous or legacy systems, ensuring robustness of AI analytics in complex environments, and maintaining reliable communications in dense or high-risk operational settings.

Respondents indicated that these risks can be mitigated through modular architectures, extensive testing in operational environments, clear governance frameworks and close collaboration with end users and regulatory authorities.

Q33. How do you consider the interoperability of the solution? Please describe how your solution addresses interoperability with existing systems, standards, platforms, or infrastructure.

Most respondents indicated that interoperability is a key design principle of their solutions. Many described the use of open standards, APIs and commonly used protocols to enable integration with existing command-and-control systems, CCTV platforms, emergency management systems and other operational infrastructures.

Several respondents also highlighted modular or microservice-based architectures and the use of middleware or gateways to ensure compatibility with heterogeneous and legacy systems. Overall, the answers confirm that interoperability with existing infrastructures is widely considered essential for the SHIELD PCP solution.

Q34. Based on your market knowledge, what is the current market value (€) of comparable solutions, and what is your estimated future market value (€) of the proposed solution(s)? Please provide a brief justification for your assessment (e.g. key assumptions, market trends, or benchmarks used).

Only a subset of respondents provided quantitative estimates of market value, while many provided qualitative observations regarding market trends and pricing models. Among the respondents who provided estimates, current deployments of comparable crowd-management or situational-awareness solutions were typically described as ranging from tens of thousands to several hundred thousand euros per site, depending on system complexity, number of sensors and level of integration required.

For larger or highly integrated deployments incorporating advanced analytics, multi-sensor integration and operational command platforms, some respondents indicated that system costs could reach several hundred thousand euros or more per deployment, often combined with annual maintenance or subscription models.

Future market projections provided by respondents suggested that demand for integrated crowd-management and public-space protection solutions is expected to increase significantly in the coming years, driven by the growing need for enhanced situational awareness, improved public-safety capabilities and compliance with emerging regulatory frameworks. Respondents also noted that market value will depend strongly on deployment scale, operational context and the level of integration with existing infrastructures.

Q35. Did you already take part in a European project, or has the development of your solution / technology been co-funded by the European Union? If so, please provide the name of the project, the Grant Agreement number and some further information.

Several respondents indicated that their organisations have previously participated in EU-funded research and innovation projects or have developed related technologies with support from European funding programmes. These projects typically focused on areas such as artificial intelligence, data analytics, crisis management platforms, cybersecurity, IoT interoperability and situational awareness systems.

The responses suggest that a portion of the technologies proposed for SHIELD PCP may build upon results and experience gained through previous European research initiatives. This indicates that the SHIELD PCP procurement can benefit from an existing base of validated research results and technological developments that could be further matured and integrated through the PCP process.

Q36. How did you hear about the project SHIELD PCP?

- ☐ Project website (shieldpcp.eu)
- ☐ Tenders Electronic Daily (TED)
- ☐ European Commission / Horizon Europe communication channels
- ☐ Partner organisation or consortium member
- ☐ Social media (LinkedIn, X/Twitter, etc.)
- ☐ Event, workshop or webinar
- ☐ Email newsletter or mailing list
- ☐ Other (please specify)

Respondents most frequently learned about the project through partner organisations or consortium members, email newsletters or mailing lists, and the SHIELD PCP project website.

Other channels included European Commission communication platforms, social media and project-related events such as webinars and workshops.

Q37. Do you have any suggestions and/or remarks?

Only a limited number of respondents provided additional remarks or suggestions at the end of the questionnaire, while the majority left this field blank. Among the comments provided, respondents suggested clarifying certain technical and regulatory aspects of the pilots, including more detailed information about operational conditions at pilot sites and clearer guidance on regulatory constraints that may apply to certain sensing or monitoring technologies.

Some respondents also encouraged continued dialogue between public buyers and potential suppliers during the preparation of the PCP tender, emphasising the importance of ensuring that technical requirements remain aligned with operational realities and technological capabilities. Overall, these comments reinforce the importance of maintaining transparent communication and clear technical specifications in the preparation of the forthcoming procurement process.

4. Conclusions

The SHIELD Open Market Consultation (OMC) provided a valuable forum for engaging public security authorities, research organisations and technology providers across Europe, gathering critical insights into operational challenges, emerging

technological capabilities and the market readiness for innovative solutions addressing the protection of public spaces and crowd management in complex operational environments. The consultation successfully validated the consortium's central assumption that there is both strong interest and significant technological capacity within the market to innovate and deliver solutions addressing the challenges defined in the SHIELD PCP use cases.

The OMC demonstrated that the market already offers a wide range of relevant technological building blocks, including crowd analytics, AI-based situational awareness, multi-sensor integration, command-and-control platforms, secure communications and drone detection capabilities. However, the consultation also confirmed that no single existing solution currently covers the full scope of the SHIELD PCP challenge. Instead, most suppliers indicated that future solutions will likely consist of modular combinations of specialised components integrated into interoperable platforms capable of supporting multi-agency operations.

The Request for Information (RFI) process revealed a strong level of interest from the market in participating in the future PCP procurement. The majority of respondents indicated their intention to participate in the upcoming tender, and many expressed a preference for forming consortia with complementary partners in order to combine expertise across different technological domains. This confirms that the SHIELD PCP procurement is likely to attract a competitive and diverse set of suppliers capable of developing innovative solutions.

While many respondents reported relatively mature technological components, the responses also highlighted important areas where further innovation and integration efforts are required. In particular, respondents identified crowd-behaviour analytics, AI-supported decision-making, multi-source data fusion and cross-agency interoperability as areas where significant development and integration work will be needed to achieve fully operational solutions.

The consultation also provided important insights into the practical challenges associated with implementing integrated solutions in real operational environments. Respondents frequently highlighted the complexity of integrating heterogeneous data sources and legacy systems used by different public-safety organisations. As a result, interoperability, open standards and flexible integration architectures were repeatedly emphasised as key design requirements for future solutions.

Providers also raised several important considerations that should be taken into account when finalising the procurement strategy. These include the need to ensure strong compliance with legal and ethical frameworks, particularly regarding data protection, privacy and the responsible use of artificial intelligence in public-space security contexts. Respondents stressed the importance of privacy-by-design approaches, human oversight in operational decision-making and clear governance frameworks for the management and sharing of operational data.

Another important observation concerns the development effort and cost structure associated with integrated solutions. The responses suggest that the prototype development and system integration phase is likely to require the greatest level of technical effort and resources, reflecting the complexity of combining multiple sensing, analytics and communication technologies into a coherent operational

system. This insight will be considered when finalising the PCP phase structure and budget allocation.

Respondents also emphasised the importance of ensuring clear and realistic technical specifications, particularly regarding pilot environments, existing infrastructure and operational validation scenarios. Several suppliers indicated that detailed information on integration conditions, technical constraints and operational requirements would facilitate more robust planning and more effective participation in the future PCP.

Overall, the OMC confirmed the relevance and feasibility of the SHIELD PCP challenge while providing valuable market feedback that will support the refinement of the future procurement. The insights gathered through the webinars, the Paris hybrid event and the RFI questionnaire will be taken into account by the consortium when finalising the PCP documentation and preparing the Call for Tender, with the objective of ensuring that the procurement framework remains realistic, competitive and conducive to innovation.

Annex 1. Microsoft Teams polling results (language-specific webinars)

This annex presents the detailed quantitative results of the Microsoft Teams polls conducted during the language-specific webinars. For each polling question (Q1-Q10) and each language session (Spanish, French, Slovak, Polish and Italian), the annex reproduces the original Microsoft Teams chart showing the number and percentage of responses per answer option. These figures complement the aggregate summaries provided in Section 3.2.4 of the report.

The structure of this annex is as follows: for each question, the question text is recalled, followed by five figures (one per language-specific webinar). Where relevant, a brief caption indicates the language and webinar date.

Q1. Have you already responded to the Request for Information (RFI) questionnaire?

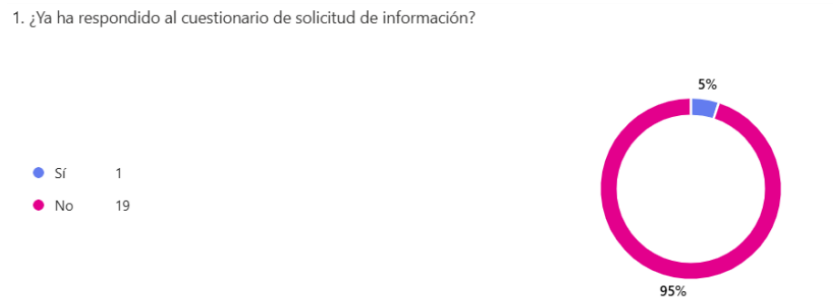


Figure A1.1 - Q1 Spanish webinar (27 January 2026) - RFI completion status

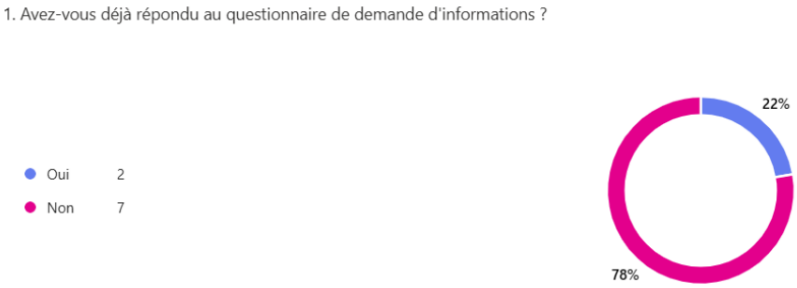


Figure A1.2 - Q1 French webinar (27 January 2026) - RFI completion status

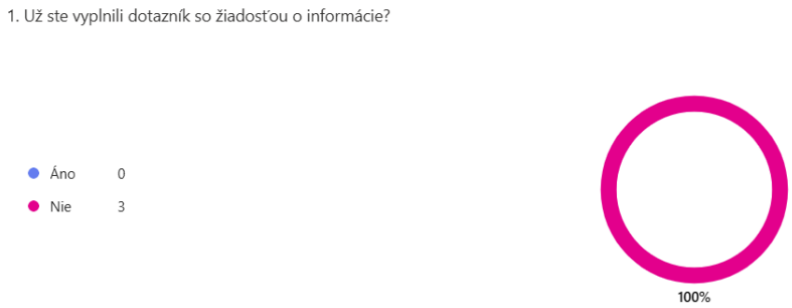


Figure A1.3 - Q1 Slovak webinar (28 January 2026) - RFI completion status

Figure A1.4 - Q1 Polish webinar (29 January 2026) - RFI completion status

Figure A1.5 - Q1 Italian webinar (29 January 2026) - RFI completion status

Q2. In the stadium panic scenario shown, at which phase could your solution contribute the most?

Figure A1.6 - Q2 Spanish webinar (27 January 2026) - Stadium panic scenario

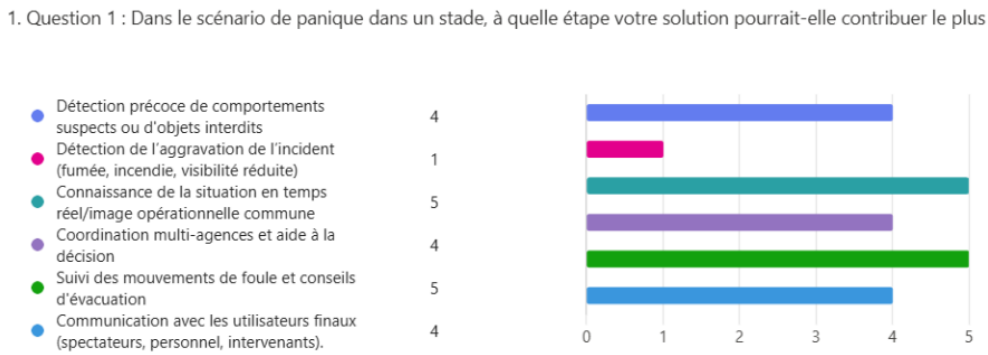


Figure A1.7 - Q2 French webinar (27 January 2026) - Stadium panic scenario

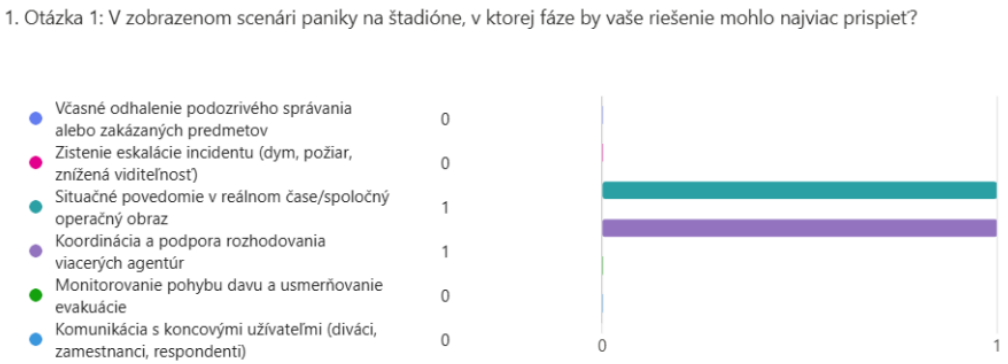


Figure A1.8 - Q2 Slovak webinar (28 January 2026) - Stadium panic scenario

Figure A1.9 - Q2 Polish webinar (29 January 2026) - Stadium panic scenario

Figure A1.10 - Q2 Italian webinar (29 January 2026) - Stadium panic scenario

Q3. For this pilot project, how would you position your contribution?

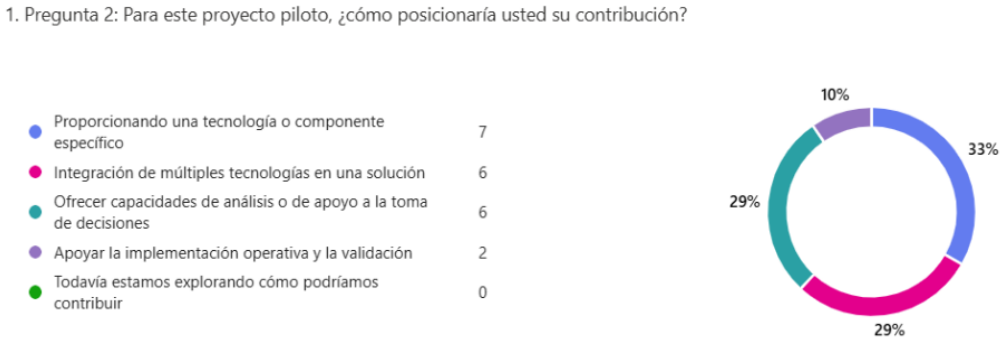


Figure A1.11 - Q3 Spanish webinar (27 January 2026) - Positioning of contribution

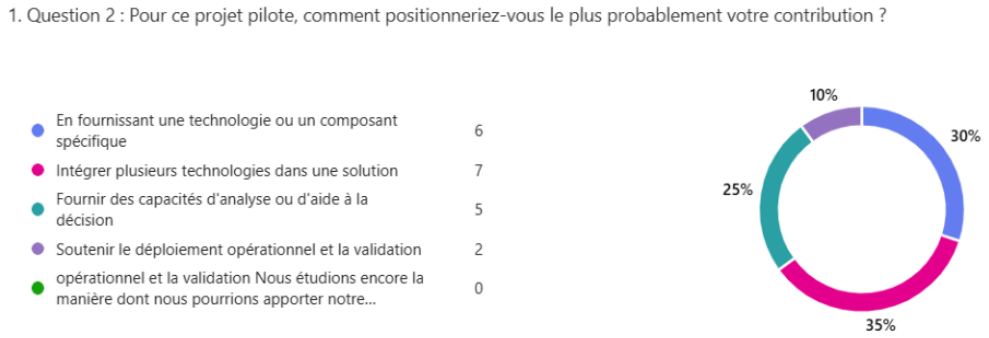


Figure A1.12 - Q3 French webinar (27 January 2026) - Positioning of contribution

Figure A1.13 - Q3 Slovak webinar (28 January 2026) - Positioning of contribution

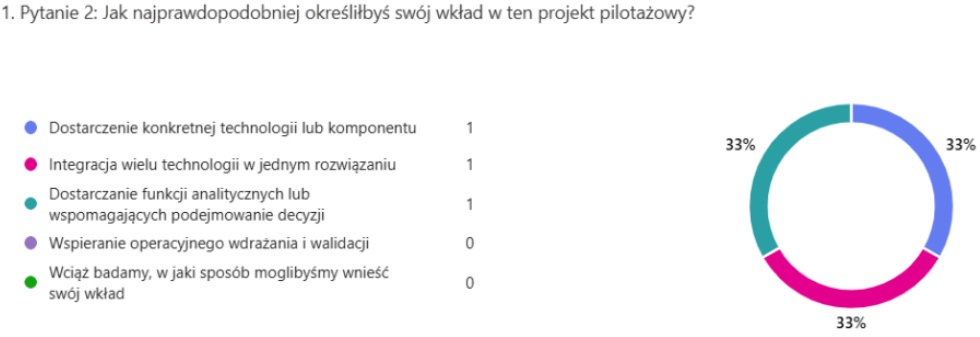


Figure A1.14 - Q3 Polish webinar (29 January 2026) - Positioning of contribution

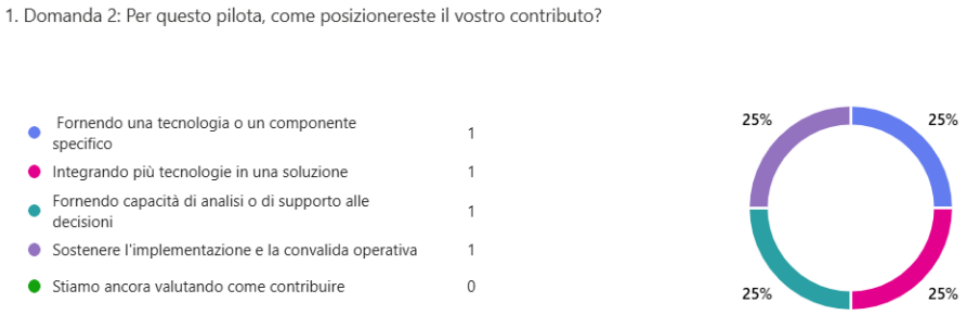


Figure A1.15 - Q3 Italian webinar (29 January 2026) - Positioning of contribution

Q4. In relation to this pilot scenario, your solution is best described as:

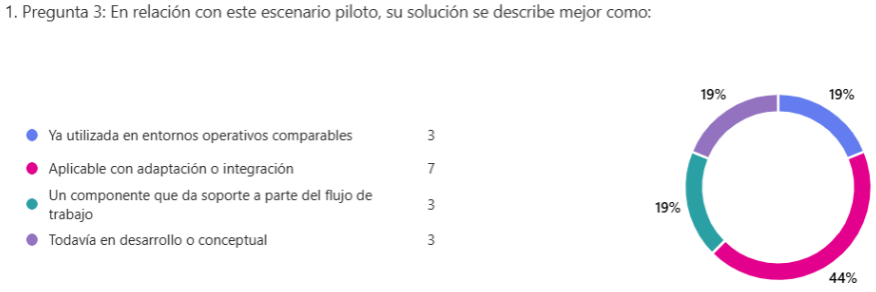


Figure A1.16 - Q4 Spanish webinar (27 January 2026) - Solution maturity

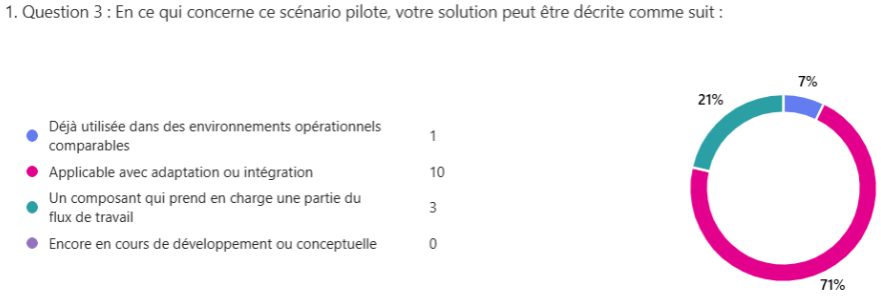


Figure A1.17 - Q4 French webinar (27 January 2026) - Solution maturity

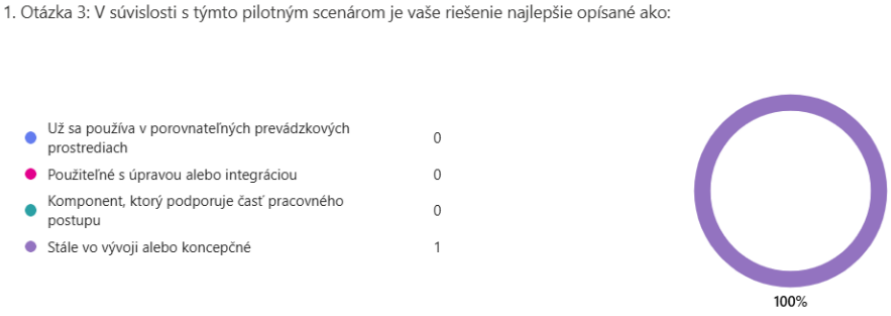


Figure A1.18 - Q4 Slovak webinar (28 January 2026) - Solution maturity

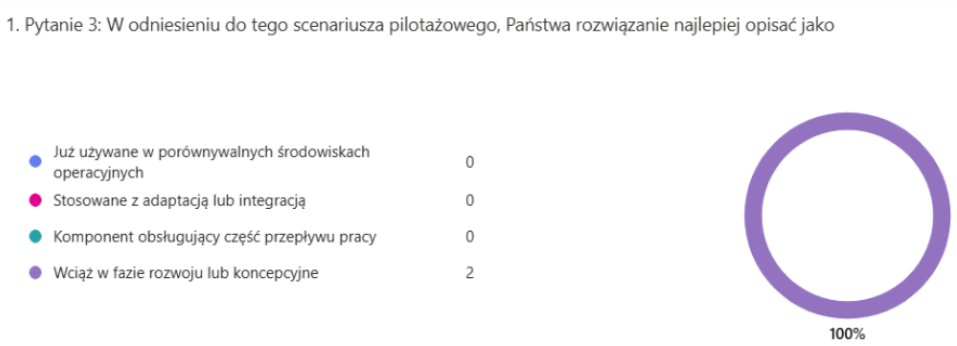


Figure A1.19 - Q4 Polish webinar (29 January 2026) - Solution maturity

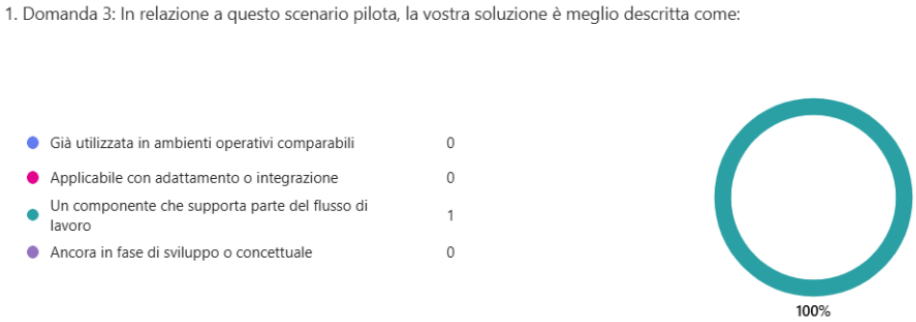


Figure A1.20 - Q4 Italian webinar (29 January 2026) - Solution maturity

Q5. In the drone attack scenario shown, at which phase could your solution contribute the most?

Figure A1.21 - Q5 Spanish webinar (27 January 2026) - Drone attack scenario

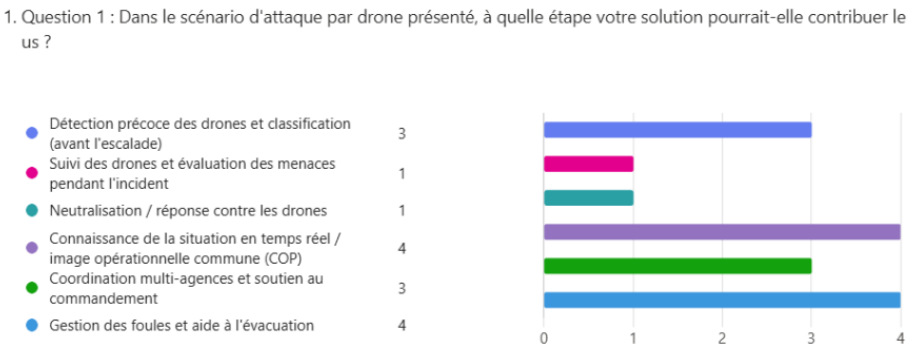


Figure A1.22 - Q5 French webinar (27 January 2026) - Drone attack scenario

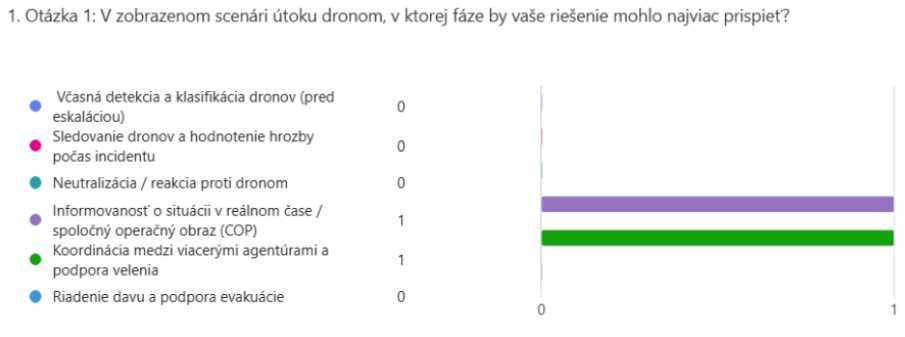


Figure A1.23 - Q5 Slovak webinar (28 January 2026) - Drone attack scenario

Figure A1.24 - Q5 Polish webinar (29 January 2026) - Drone attack scenario

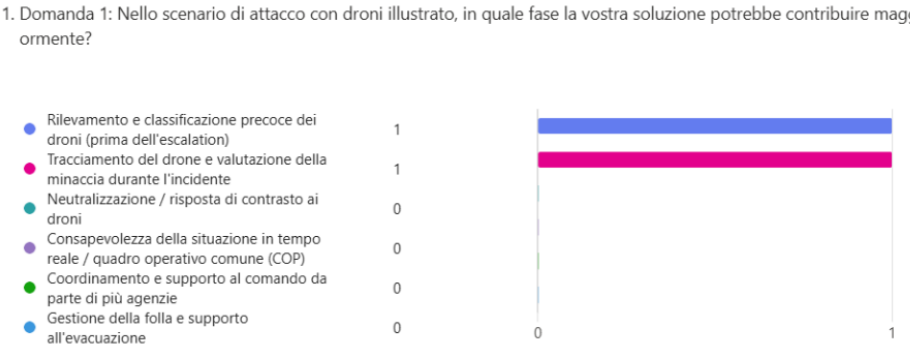


Figure A1.25 - Q5 Italian webinar (29 January 2026) - Drone attack scenario

Q6. For this pilot project, how would you position your contribution?

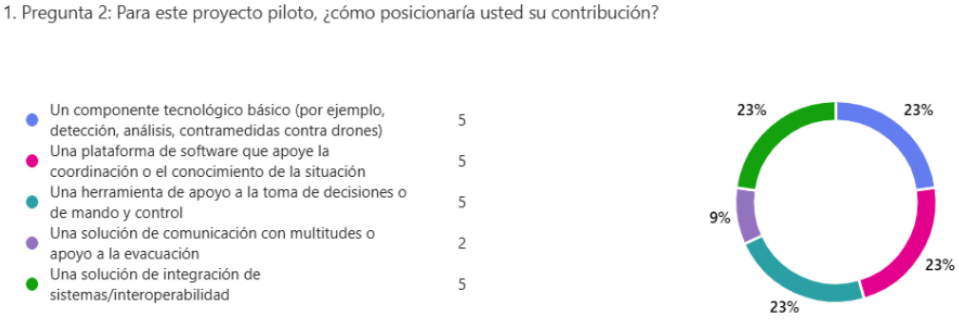


Figure A1.26 - Q6 Spanish webinar (27 January 2026) - Positioning of contribution (drone pilot)

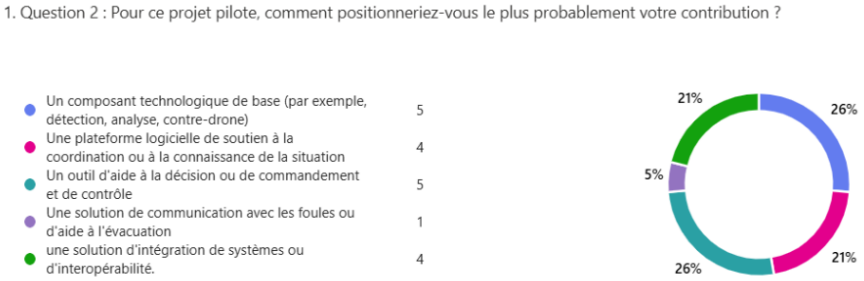


Figure A1.27 - Q6 French webinar (27 January 2026) - Positioning of contribution (drone pilot)

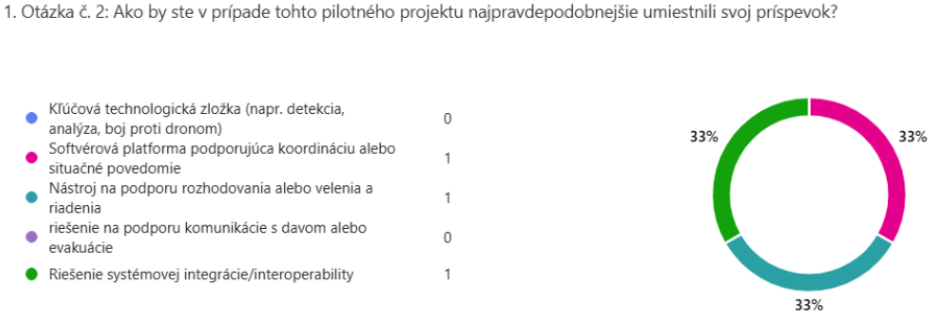


Figure A1.28 - Q6 Slovak webinar (28 January 2026) - Positioning of contribution (drone pilot)

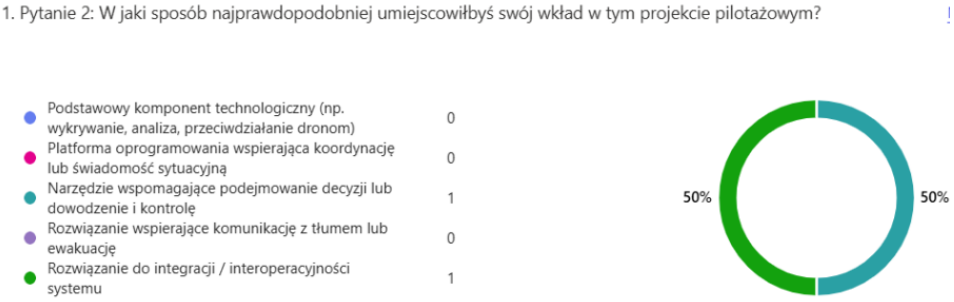


Figure A1.29 - Q6 Polish webinar (29 January 2026) - Positioning of contribution (drone pilot)

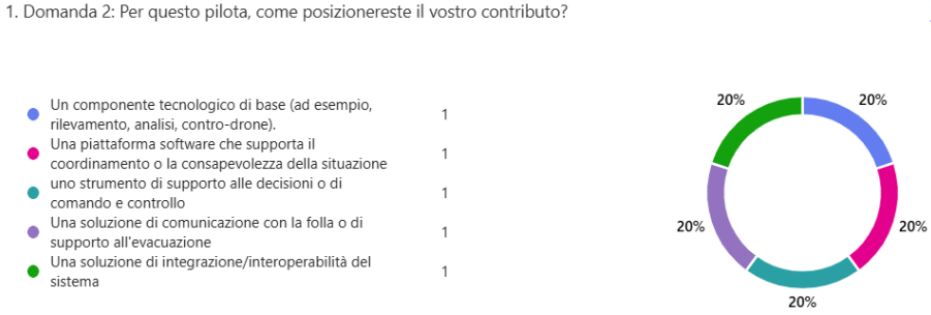


Figure A1.30 - Q6 Italian webinar (29 January 2026) - Positioning of contribution (drone pilot)

Q7. In relation to this pilot scenario, your solution is best described as:

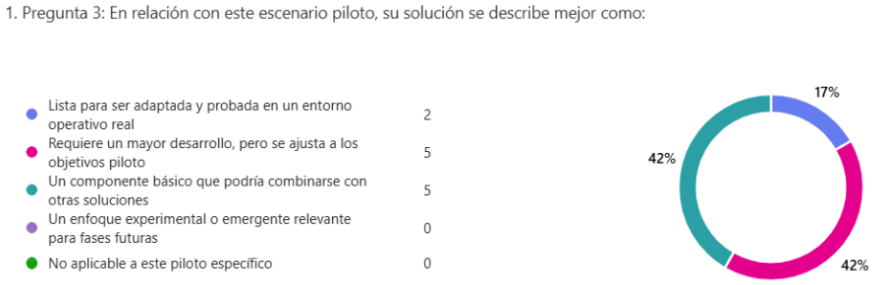


Figure A1.31 - Q7 Spanish webinar (27 January 2026) - Solution maturity (drone pilot)

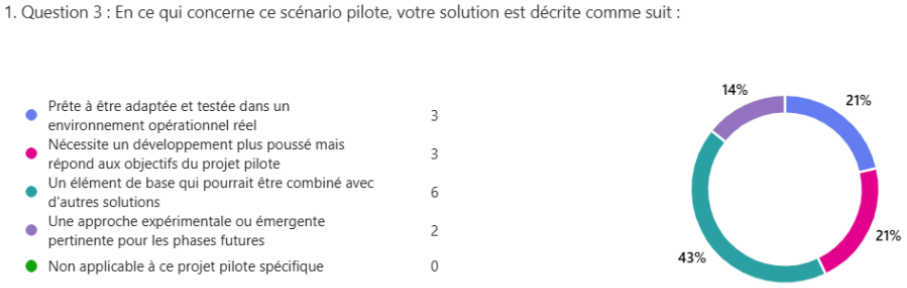


Figure A1.32 - Q7 French webinar (27 January 2026) - Solution maturity (drone pilot)

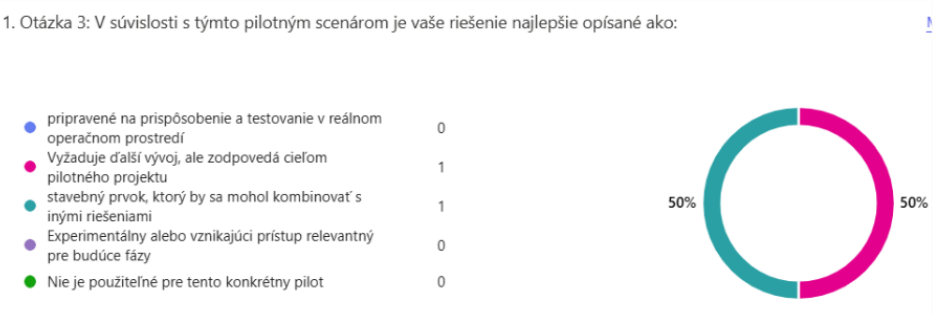


Figure A1.33 - Q7 Slovak webinar (28 January 2026) - Solution maturity (drone pilot)

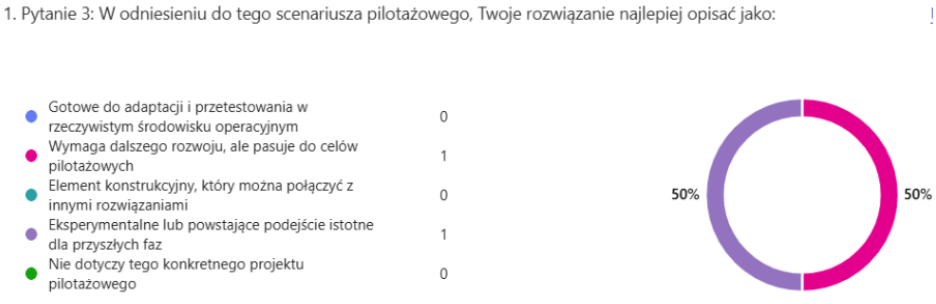


Figure A1.34 - Q7 Polish webinar (29 January 2026) - Solution maturity (drone pilot)

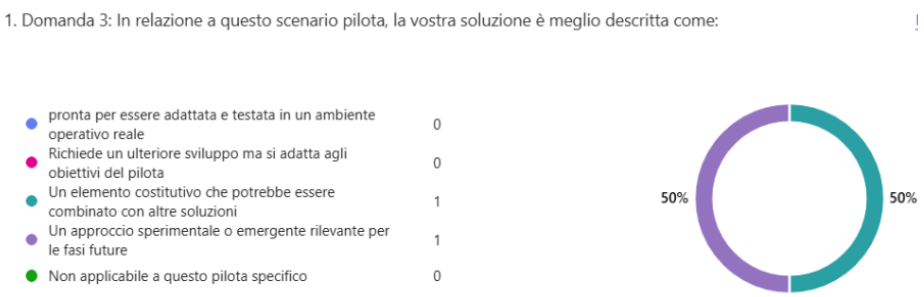


Figure A1.35 - Q7 Italian webinar (29 January 2026) - Solution maturity (drone pilot)

Q8. In the knife attack scenario shown, at which phase could your solution contribute the most?

Figure A1.36 - Q8 Spanish webinar (27 January 2026) - Knife attack scenario

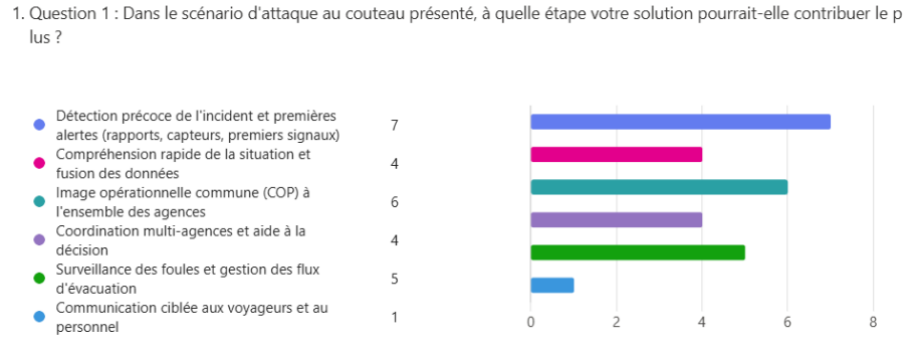


Figure A1.37 - Q8 French webinar (27 January 2026) - Knife attack scenario

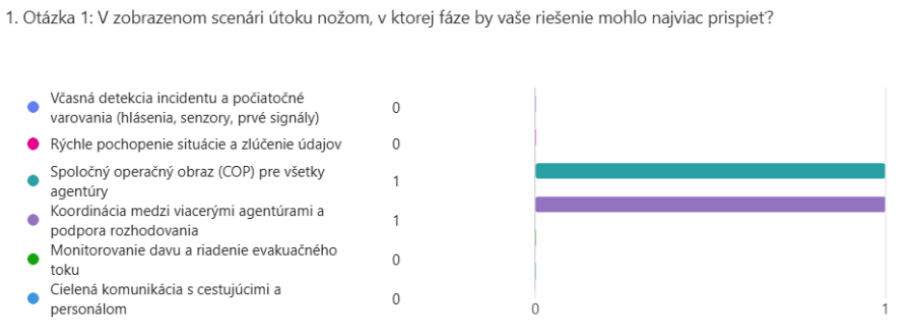


Figure A1.38 - Q8 Slovak webinar (28 January 2026) - Knife attack scenario

Figure A1.39 - Q8 Polish webinar (29 January 2026) - Knife attack scenario

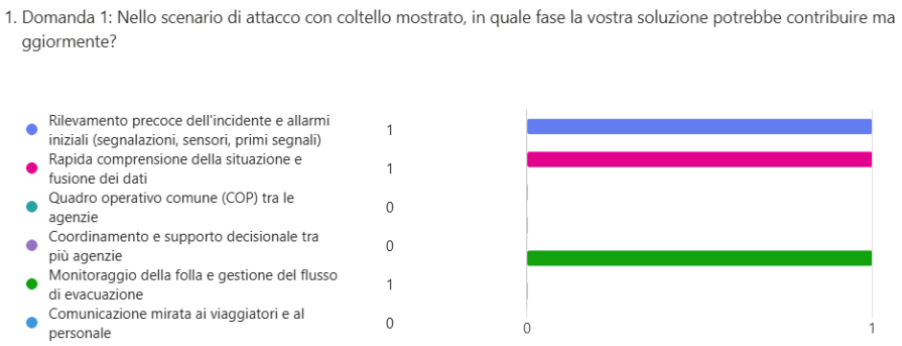


Figure A1.40 - Q8 Italian webinar (29 January 2026) - Knife attack scenario

Q9. For this pilot project, how would you position your contribution?

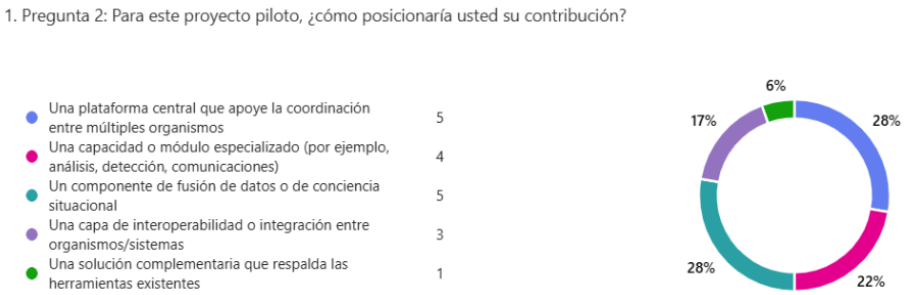


Figure A1.41 - Q9 Spanish webinar (27 January 2026) - Positioning of contribution (knife-attack pilot)

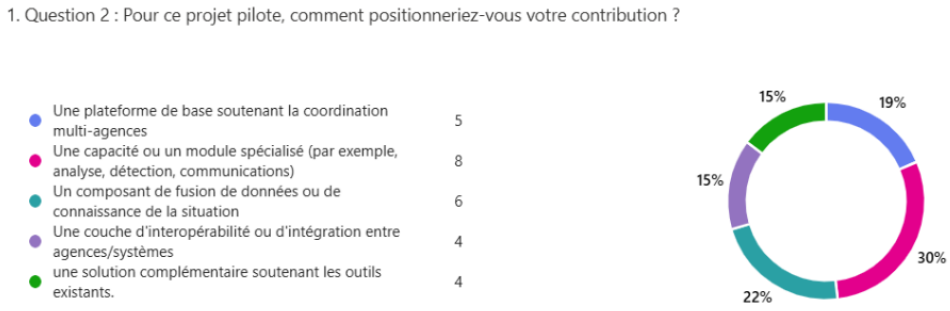


Figure A1.42 - Q9 French webinar (27 January 2026) - Positioning of contribution (knife-attack pilot)

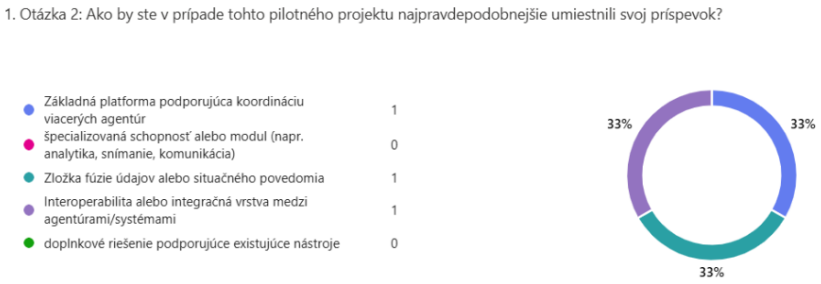


Figure A1.43 - Q9 Slovak webinar (28 January 2026) - Positioning of contribution (knife-attack pilot)

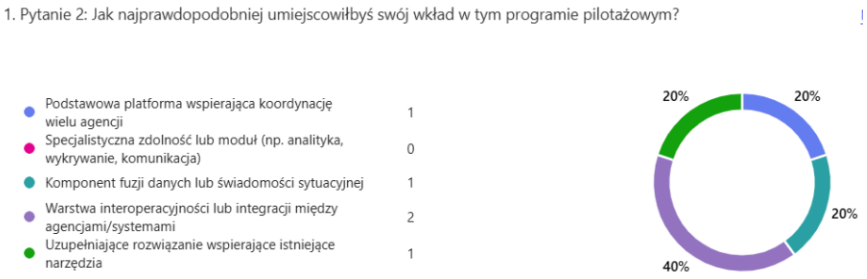


Figure A1.44 - Q9 Polish webinar (29 January 2026) - Positioning of contribution (knife-attack pilot)

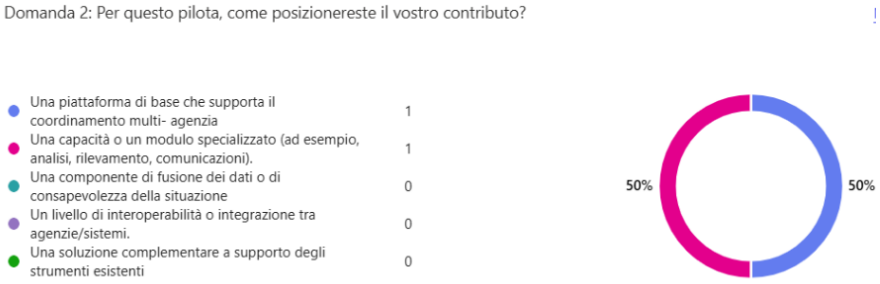


Figure A1.45 - Q9 Italian webinar (29 January 2026) - Positioning of contribution (knife-attack pilot)

Q10. In relation to this pilot scenario, your solution is best described as:

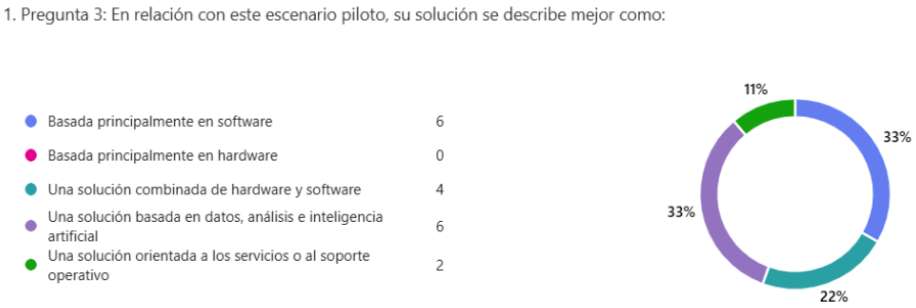


Figure A1.46 - Q10 Spanish webinar (27 January 2026) - Technical nature of solution

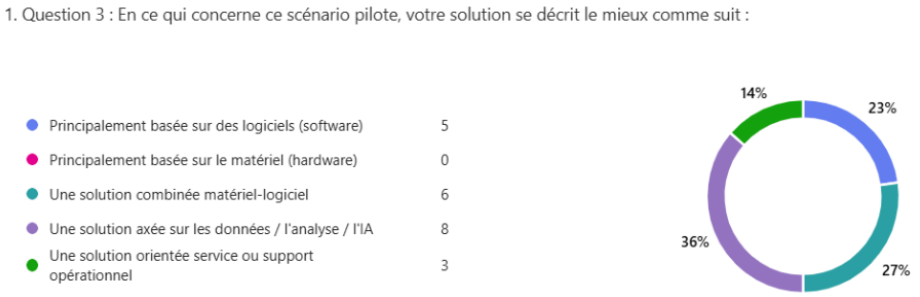


Figure A1.47 - Q10 French webinar (27 January 2026) - Technical nature of solution

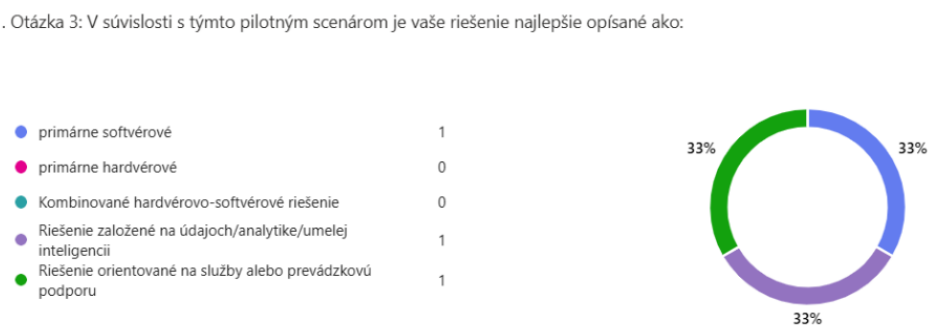


Figure A1.48 - Q10 Slovak webinar (28 January 2026) - Technical nature of solution

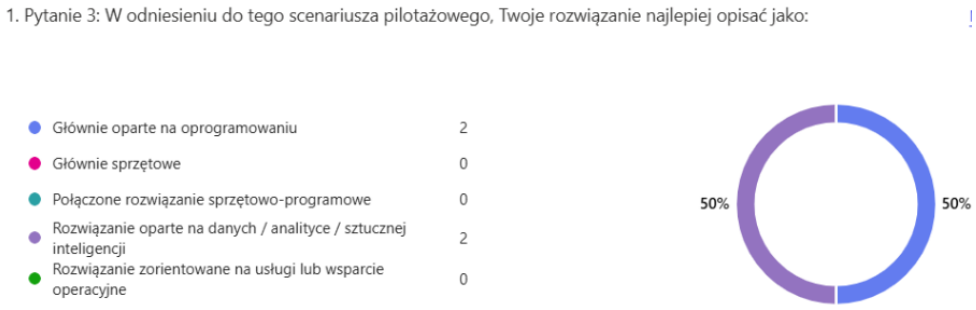


Figure A1.49 - Q10 Polish webinar (29 January 2026) - Technical nature of solution

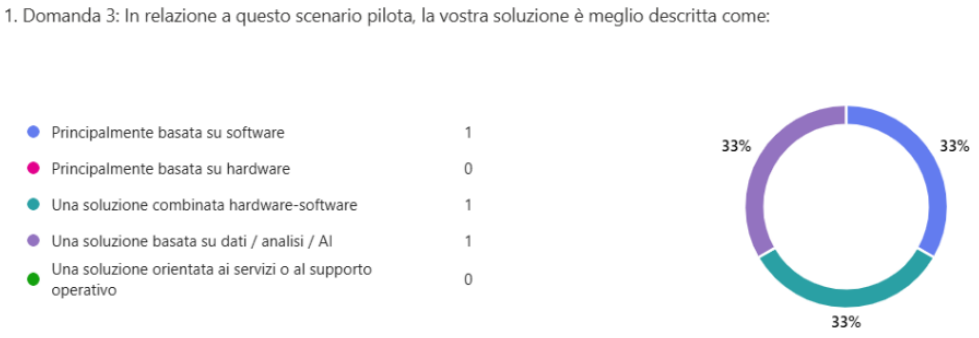


Figure A1.50 - Q10 Italian webinar (29 January 2026) - Technical nature of solution

Annex 2. Consolidated Q&A from language-specific webinars

The following pages reproduce the Q&A document as published on the SHIELD PCP website.

Questions & Answers (Q&A)

Shield PCP Open Market Consultation Activities

Q1. Does participating in the Open Market Consultation prevent a company from later submitting a proposal to the tender?

A: No. Participation in the Open Market Consultation does not prevent companies from later participating in the tender. Companies are encouraged to participate, as the consultation helps define requirements and the state of the art, but it has no impact on eligibility for the future procurement procedure.

Please note that participation in the Open Market Consultation does not provide any advantage or disadvantage to any supplier or group of suppliers.

Q2. Are there eligibility requirements to participate in the tender (e.g. minimum turnover, certifications, administrative or technical requirements)?

A: Yes. The eligibility and selection requirements will be explicitly defined in the Call for Tender documentation.

In line with standard Pre-Commercial Procurement (PCP) practice, the approach is generally to avoid imposing high financial thresholds (e.g. turnover requirements) and instead focus on the quality and technical merit of the proposal under the award criteria.

Certain evidence may be requested where relevant (for example, references from previous projects or certifications related to specific aspects of the solution). The intention is to keep barriers to participation proportionate and supportive of SMEs, while ensuring capacity to perform the contract. Final requirements will be detailed in the tender documents.

Q3. Must proposals be submitted as a consortium, and how are consortia evaluated within the PCP procedure?

A: Under PCP rules, both single entities and consortia are generally eligible to apply, unless otherwise explicitly stated in the Call for Tender.

A bidder may submit individually if it is capable of meeting all requirements alone. However, given the broad and multidisciplinary scope of the challenge, it is expected that many proposals will involve consortia bringing together complementary expertise.

In this regard, to address the full set of technical requirements, suppliers are encouraged to form consortia to increase their capacity to deliver a

comprehensive solution. The matchmaking tool available on the project's website, as well as dedicated events, are designed to facilitate partner search and consortium building. In this context, a matchmaking session will be held during the OMC event in Paris on 25 February 2026.

In a PCP procedure, bidders submit their proposed technical approach in response to the defined challenge, and proposals are evaluated as submitted. The contracting authorities do not pre-select individual components and assemble teams themselves. External entities do not formally select or label consortia within the PCP procedure. The evaluation and selection process is conducted exclusively in accordance with the procurement rules defined in the Call for Tender.

The final eligibility and participation conditions will be specified in the Call for Tender.

Q4. Can a company participate in more than one consortium or submit multiple bids?

A: Participation rules concerning multiple bids or involvement in more than one consortium will be defined in the Call for Tender.

Typically, PCP procedures include safeguards to ensure fair competition, avoid conflicts of interest, and preserve equal treatment. The exact conditions — including whether participation in multiple consortia is permitted — will be specified in the tender documents.

Q5. Is there an obligation to include companies from several EU Member States in a consortium?

A: There is generally no automatic obligation to include companies from multiple Member States unless explicitly required in the Call for Tender.

However, eligibility conditions regarding the place of establishment will apply (e.g. companies established in EU Member States or associated countries), in line with PCP and Horizon Europe rules. Detailed requirements will be clarified in the tender documents.

Q6. How can smaller companies collaborate or form consortia?

A: Collaboration is strongly encouraged, particularly for companies that cannot cover all requirements individually.

The project provides a matchmaking tool on the website (https://shieldpcp.eu/tender/#matchmaking_form), and companies completing the matchmaking form will receive a consolidated catalogue of other organisations that have also expressed interest.

In addition, dedicated matchmaking sessions are organised during the Paris event (25 February 2026) to facilitate networking, partner identification, and consortium building.

Q7. Are you looking for a complete end-to-end solution, or can partial solutions covering specific functionalities be acceptable?

A: The objective of the upcoming PCP is to procure R&D services leading to the development of a complete solution addressing the defined challenge.

However, during the Open Market Consultation phase, companies may present partial solutions, individual technologies, or specific technological contributions. These inputs are valuable and help shape the final requirements, which are still being refined.

Innovation procurement does not require starting from scratch. Existing technologies — even if developed independently — may be adapted, reused, integrated, or further developed into a final solution. The key consideration is whether the proposed approach can collectively address the identified needs.

Q8. Must a solution address all three pilots, or can it focus on only one?

A: The three pilots will be operationally tested during Phase 3, and each public buyer is associated with a specific pilot scenario.

Solutions are expected to be applicable across all pilots. However, suppliers are not expected to develop three entirely different solutions. The expectation is to propose a generic, modular and scalable solution capable of responding to common operational needs shared across the pilot scenarios.

Validation activities during Phase 3 are expected to take place across the different pilots rather than being limited to a single site.

Q9. Can new components be developed from scratch, and what Technology Readiness Level (TRL) is expected?

A: Yes. The PCP allows for both existing solutions and the development of new components.

The expected TRL evolves throughout the PCP phases:

- Phase 1 – Solution Design: approx. TRL 3–4
- Phase 2 – Prototype Development: approx. TRL 5–6
- Phase 3 – Operational Validation: approx. TRL 7–8

Prototypes developed in later phases will be tested in real operational environments. It is possible — and often expected — to combine market-ready components with newly developed elements, particularly where integration is a key innovation gap.

Q10. Some components may already have a high TRL or be partially deployed. Is this an issue in a PCP?

A: No. The PCP does not require that every component be at a low TRL.

Innovation may lie in integration, adaptation, scaling, or combining existing technologies in new ways. What matters is the ability to advance the overall solution, address the defined operational needs, and contribute to the targeted TRL progression.

Q11. Is facial recognition or the use of biometric data required?

A: No. Facial recognition is not imposed as a requirement and is not mandatory. Providers are free to propose their own approaches.

Any use of biometric data must strictly comply with European and national legal frameworks, including GDPR. In several contexts, such use is highly restricted or prohibited, particularly for certain operators.

Legal and ethical analyses will be conducted for each pilot and country. If the processing of biometric data is not permitted in a given jurisdiction (for example, in France), such functionality will not be tested in that pilot site.

Q12. How will broader privacy constraints and differing national interpretations be addressed?

A: Solutions are expected to comply with GDPR and all relevant legal frameworks.

Where possible, minimising the use of biometric or personal data is preferable. Bidders must demonstrate compliance and propose an approach that remains legally sound across different national contexts.

Real-life deployments typically require a Data Protection Impact Assessment (DPIA). The legal framework, particularly regarding algorithmic video surveillance, is evolving at both national and European levels. This evolving regulatory context is one of the reasons why the PCP initiative is relevant.

Q13. Who will operate drone neutralisation tools?

A: Drone neutralisation is currently foreseen only within the Spanish pilot scenario.

Such tools would be operated exclusively by authorised national authorities involved in that pilot. Not all actors are legally permitted to operate such equipment. Responsibilities and operational arrangements will be clarified with the competent authorities.

Q14. How many providers will be selected in each PCP phase?

A: The PCP follows a competitive funnel approach:

- Phase 1: approximately 4–5 providers
- Phase 2: approximately 3 providers
- Phase 3: at least 2 providers

The exact number depends on the number and quality of proposals received and the evaluation results. Contractors are invited to submit a proposal for the next phase only if their performance in the previous phase is successfully evaluated.

Evaluation criteria and procedures will be detailed in the tender documents.

Q15. Is the PCP competitive or collaborative?

A: The PCP is competitive in nature. Suppliers or consortia develop their solutions in parallel, and the best-performing ones are invited to submit a proposal for the next phase.

There may be structured interaction with end-users, including periodic meetings or feedback moments, but progression between phases is based on competitive evaluation results.

Q16. How will evaluation be handled if different solutions cover different parts of the requirements?

A: At the time of the webinars, the evaluation criteria and weighting were not yet fully finalised.

The complete evaluation framework — including award criteria and weighting — will be defined and published in the Call for Tender documentation. Once launched, all applicants will have access to the evaluation methodology.

Q17. What is the final objective of the PCP?

A: The PCP is designed to support TRL progression and the development of mature, validated solutions suitable for future large-scale procurement.

It is not intended for immediate large-scale deployment. Instead, it supports development, integration, and validation in operational environments.

The PCP should also be viewed within the broader EU innovation framework, potentially paving the way for a future Public Procurement of Innovative solutions (PPI) involving multiple public buyers across Europe and supporting the creation of a European market for security solutions.

Q18. What is the total budget and the distribution per phase?

A: The total project budget is EUR 3,600,000.

The indicative distribution between phases is:

- Phase 1 – Solution Design: €450,000
- Phase 2 – Prototype Development: €2,250,000
- Phase 3 – Operational Validation: €900,000

The budget of each phase is divided among the selected contractors based on their financial proposals.

For all phases, contracts will be financed until the remaining budget is insufficient to fund the next best tender. The exact number of contracts finally awarded will thus depend on the prices offered and the number of tenders passing the evaluation.

Q19. Is research and experimentation funded?

A: Yes. Research and experimentation are funded within the PCP:

- Phase 1 focuses on solution design
- Phase 2 on prototype development
- Phase 3 on operational experimentation and testing in real environments

All phases are covered by PCP funding, subject to contractual conditions.

Q20. How will intellectual property rights be handled?

A: At this stage, the IP conditions are not yet fully defined. Based on standard PCP practice, intellectual property typically remains with the suppliers developing that generate it, not with the consortium.

In return, public buyers may receive usage rights or licences for the final solution, depending on the final IPR distribution model. The exact arrangements will be specified in the Call for Tender.

Q21. Is there any preference for patented solutions? Is patenting required?

A: There is no requirement or preference that bidders must already have patents. Patents were used in the project's analysis mainly to understand the state- of- the- art and overall innovation landscape.

Q22. Can the questionnaire be submitted multiple times?

A: The organisations should submit one answer. If an organisation has multiple solutions, these can be described within a single submission using the open text fields.

Q23. How is confidentiality ensured for questionnaire responses?

A: All responses provided by market parties will be anonymised and treated as confidential.

The SHIELD PCP consortium will not disclose specific answers from individual operators. Only general findings and a summary of responses will be published in an anonymous report on the project website.

Q24. What is the objective of the hybrid event (25 February)?

A: The hybrid OMC event aims to present the SHIELD PCP project and facilitate structured dialogue between public buyers and potential suppliers ahead of the forthcoming Call for Tender.

The event relevant to suppliers takes place on 25 February (the 26 February session is reserved for consortium members).

The agenda includes:

- Welcome and project introduction (rationale, use cases, PCP process)
- Presentation of the state-of-the-art analysis
- Overview of the Open Market Consultation (OMC) objectives and activities
- Interactive session with participants
- Presentation of next steps
- A dedicated matchmaking session (aiming at creating dynamics among participants to facilitate consortium building), including supplier presentations and bilateral exchanges

The objective is to clarify the challenge, gather market feedback, and support networking and potential partnerships among interested stakeholders.

Q25. Will the participant list be published?

A: The participant list will not be publicly published.

Registered participants may access information about other participants for matchmaking purposes, subject to consent.

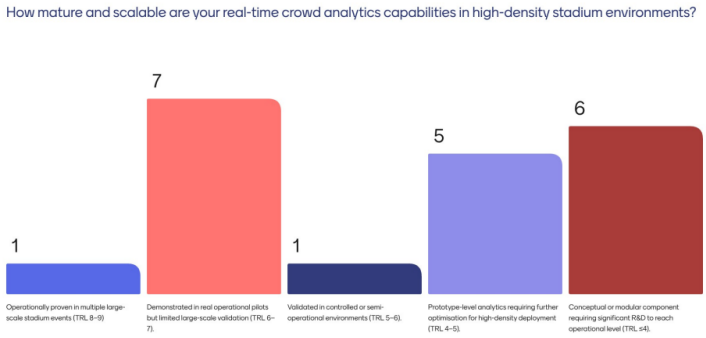
Q26. What happens after completing the matchmaking form?

A: Companies that complete the matchmaking form will receive a consolidated catalogue of other organisations that have also filled it in.

Dedicated matchmaking sessions during the Paris event further support consortium building.

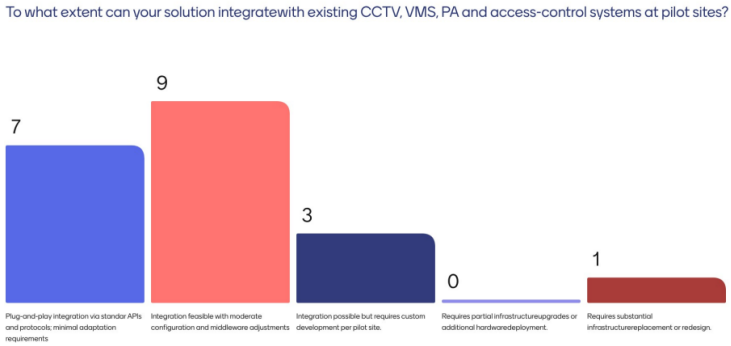
Annex 3. The results of the interactive session on 25 February 2026

Q1. How mature and scalable are your real-time crowd analytics capabilities in high-density stadium environments?



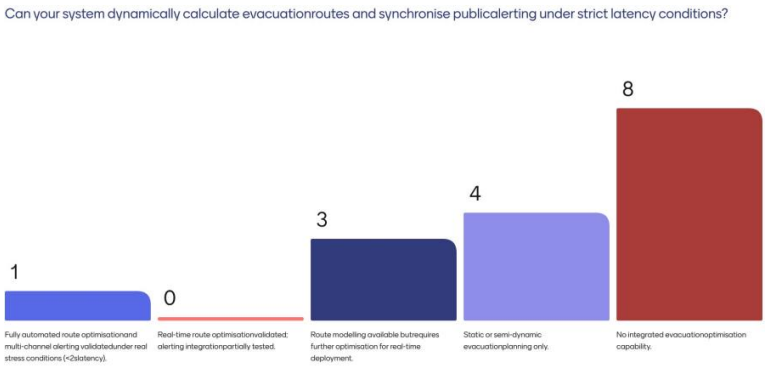
For real-time crowd analytics in high-density stadium environments, only 1 participant reported fully operational, large-scale deployment at TRL 8-9, while the majority positioned themselves at TRL 6-7 or below, including 5 at prototype-level (TRL 4-5) and 6 at conceptual or modular stage (TRL ≤4).

Q2. To what extent can your solution integrate with existing CCTV, VMS, PA and access-control systems at pilot sites?



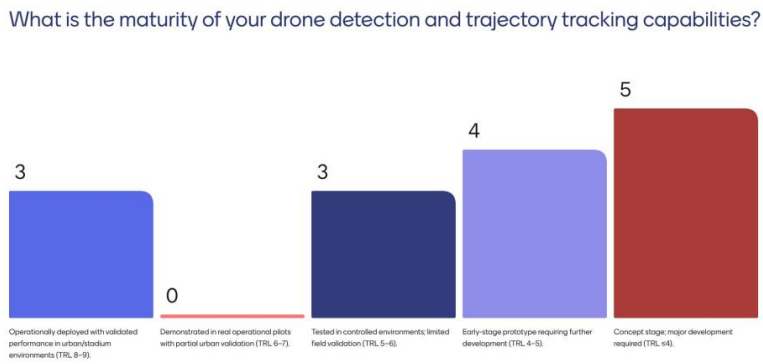
For integration with existing CCTV, VMS, PA and access-control systems, 7 respondents indicated plug-and-play integration via standard APIs and 9 reported integration feasible with moderate configuration, while only 1 saw a need for substantial infrastructure replacement.

Q3. Can your system dynamically calculate evacuation routes and synchronise public alerting under strict latency conditions?



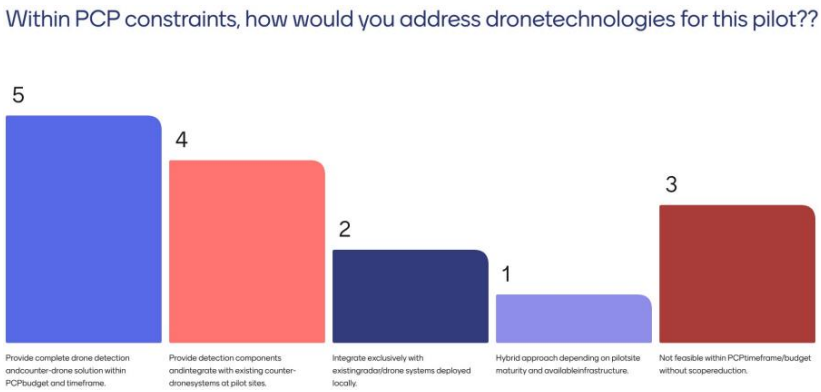
On dynamic evacuation routing and synchronised public alerting, 8 participants declared having no integrated evacuation optimisation capability and 4 only static or semi-dynamic planning, whereas just 1 reported fully automated optimisation and multi-channel alerting validated under stress.

Q4. What is the maturity of your drone detection and trajectory tracking capabilities?



For drone detection and trajectory tracking, 3 respondents reported operational deployments in urban/stadium environments at TRL 8-9, while the majority were at earlier stages (3 at TRL 5-6, 4 at TRL 4-5 and 5 still at concept level).

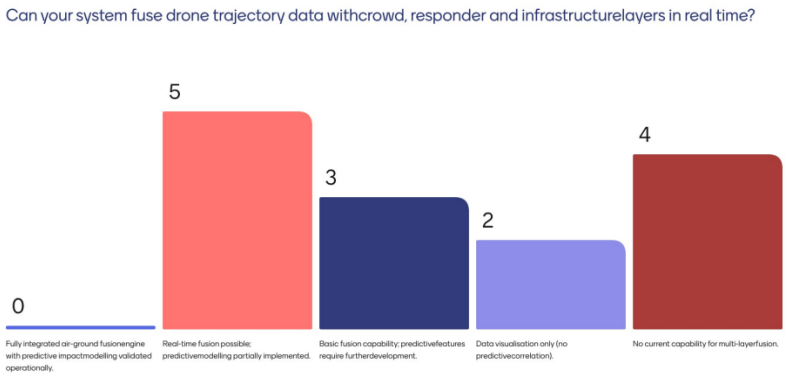
Q5. Within PCP constraints, how would you address drone technologies for this pilot?



When asked how they would address drone technologies within PCP constraints, 5 participants aimed to provide a complete detection and counter-drone solution, 4 preferred supplying detection components integrated with existing systems, and 3

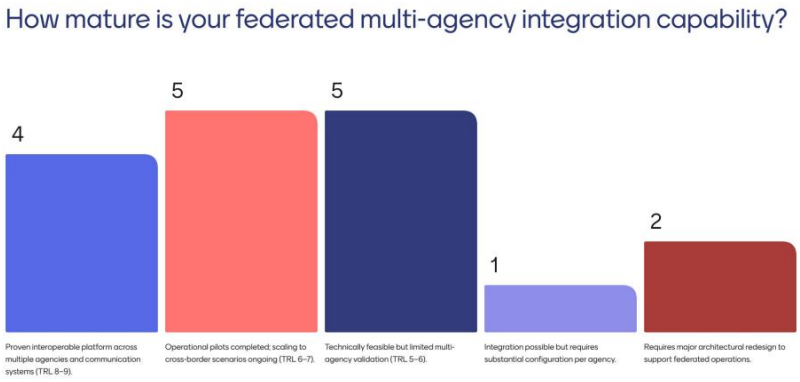
considered that such capabilities would not be feasible within the PCP timeframe and budget without scope reduction.

Q6. Can your system fuse drone trajectory data with crowd, responder and infrastructure layers in real time?



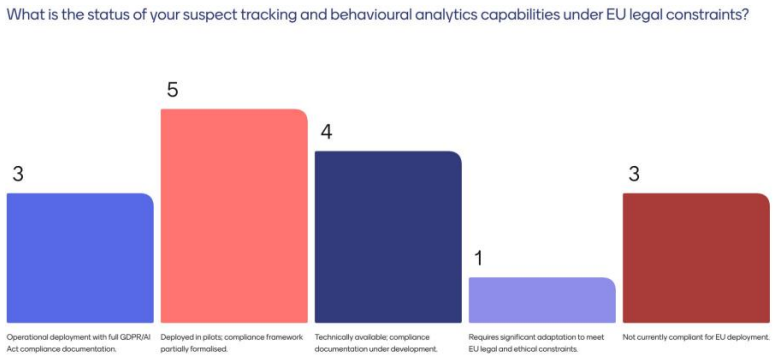
For real-time fusion and drone trajectories with crowd, responder and infrastructure layers, 5 respondents reported real-time fusion with partially implemented predictive modelling, while 4 stated that they currently have no multi-layer fusion capability and the remainder indicated only basic fusion or visualisation-only approaches.

Q7. How mature is your federated multi-agency integration capability?



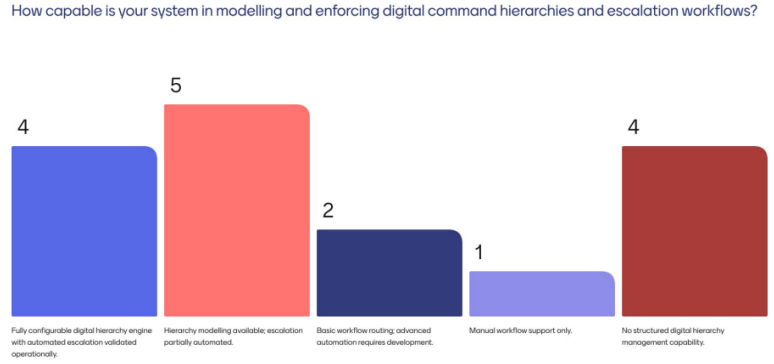
On federated multi-agency integration, 4 participants reported proven interoperable platforms across multiple agencies (TRL 8-9), 10 located themselves between TRL 5-7 (from limited validation to ongoing cross-border pilots), and 2 indicated that major architectural redesign would be needed.

Q8. What is the status of your suspect tracking behavioural analytics capabilities under EU legal constraints?



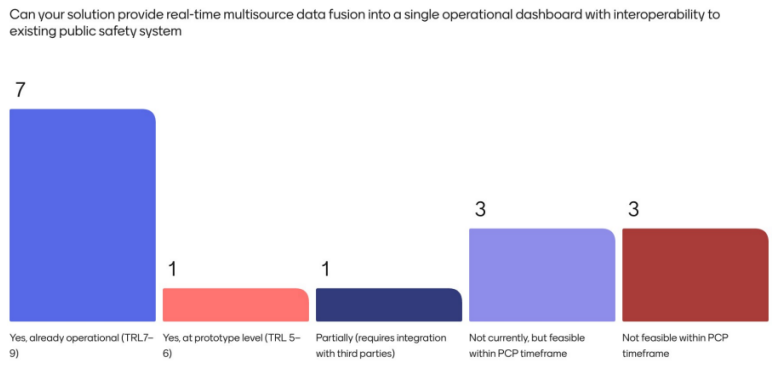
Regarding suspect tracking and behavioural analytics under EU legal constraints, 8 respondents indicated deployed or pilot solutions with at least partially formalised compliance (3 fully documented; 5 partially), while 3 stated that their current solutions are not compliant and 1 foresaw significant adaptations.

Q9. How capable is your system in modelling and enforcing digital command hierarchies and escalation workflows?



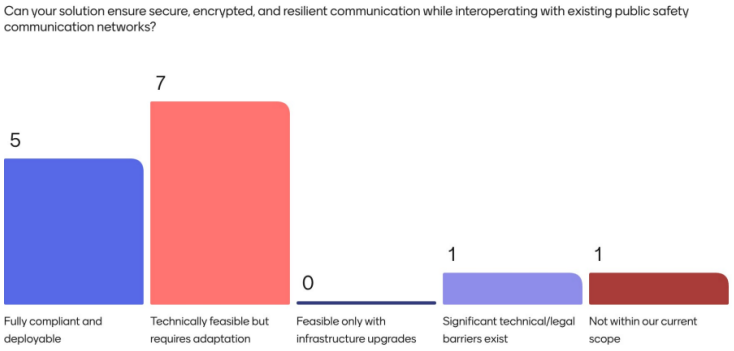
On digital command hierarchies and escalation workflows, 9 respondents reported at least partial automation (4 fully configurable engines with automated escalation and 5 with partial automation), whereas 6 indicated only basic or manual workflows and 4 had no structured hierarchy management at all.

Q10. Can your solution provide real-time multisource data fusion into a single operational dashboard with interoperability to existing public safety systems?



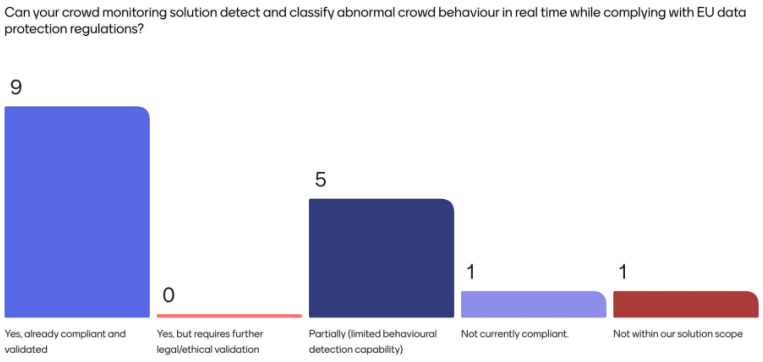
For multi-source data fusion into a single operational dashboard, 7 participants already had operational capabilities at TRL 7-9, while 3 considered such dashboards not feasible within the PCP timeframe and the remainder were at prototype or partial-integration stages.

Q11. Can your solution ensure secure, encrypted, and resilient communication while interoperating with existing public safety communication networks?



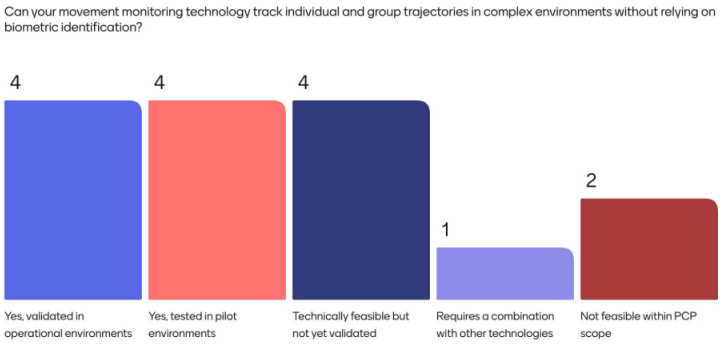
On secure, encrypted and resilient communication interoperable with existing public-safety networks, 5 respondents reported fully compliant and deployable solutions, 7 saw their solutions as technically feasible but requiring adaptation, and only 2 pointed to major barriers or out-of-scope functionality.

Q12. Can your crowd monitoring solution detect and classify abnormal crowd behaviour in real time while complying with EU data protection regulations?



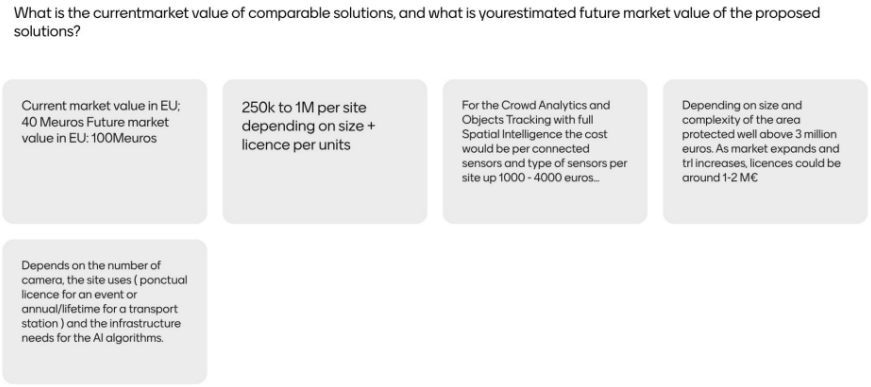
For abnormal crowd-behaviour detection under EU data-protection rules, 9 participants reported solutions already compliant and validated, 5 indicated only partial behavioural detection capability, and 2 had no compliant solution in scope.

Q13. Can your movement monitoring technology track individual and group trajectories in complex environments without relying on biometric identification?



For non-biometric movement monitoring, 8 participants reported validated capabilities in operational or pilot environments, 4 were at the stage of technical feasibility without full validation, and 2 considered such tracking not feasible within the PCP scope.

Q14. What is the current market value of comparable solutions, and what is your estimated future market value of the proposed solutions?



A final open poll on current and future market value yielded qualitative estimates ranging from hundreds of thousands of euros per site to several million euros for large deployments, as well as broader EU-level market projections (for example, from tens to around one hundred million euros). These responses illustrate that participants perceive a wide pricing range depending on what size, deployment model (even-based versus permanent), and required infrastructure for AI and analytics.