EU Horizon 2020 Research & Innovation Program
Advanced Robot Capabilities & Take-Up
ICT-25-2016-2017
Grant Agreement No. 779942

Safe Robot Navigation in Dense Crowds

http://www.crowdbot.org

Technical Report

D 1.2: Experiment Protocol & Risk Assessment

Work Package 1 (WP 1)
Scenarios Co-Design & Evaluation

Task Lead: University College London, UK
WP Lead: University College London, UK

Table of Contents

Executive Summary

As part of external stakeholder engagements, two types of experiments —user studies and robotic tests— are planned for the Crowdbot project. User studies are further classified as structured interviews and focus group engagements. Both user study experiments will be used to collect information and better understand the viewpoints and concerns of various stakeholders that will be exposed to our robots. Some examples of these stakeholders are potential users of our robots, robotic experts, property owners and venue managers whose space our robots may likely roam and members of the general public that will interact with robots. Several rounds of user studies are planned over the duration of the project. They work in tandem with robotic tests in several rounds interview-test-interview cycles. Data collected from user studies assist the test team in selecting specific types of robotic test cases that are most meaningful and relevant to the main project goal of safe navigation of robots among dense human crowds. After completion of robotic tests, collected data is then used to inform stakeholders of observed robot-human interactions and to solicit their feedback in the next round of user studies.

Robotic tests are experiments in which a Crowdbot robot is programmed to roam around a high density of human crowds in diverse physical environments such as the hospital floor, train station platforms, airport departure gate areas or office corridors. The success of such robotic tests rest on a number of factors: recruitment of human participants, reservation of test venue, planning and well execution of test cases. Risk mitigation procedures should also be in place to anticipate unforeseen events or deviation from scripted test cases.

This report covers two important aspects of experiments: protocol and risk assessment. As background material, in Section 1 we explain the classification of external stakeholders into seven main classes. Section 2 we provide a summary of material resources and venue spaces that will be reserved and utilized in each experiment. Sections 3 and 4 cover details of logistics planning and experiment procedures for both user studies and robotic tests, respectively. Section 5 addresses the important topic of human participant recruitment.

Section 6 covers various topics associated with risk assessment. Several types of risks are anticipated when conducting robotic tests, and to a lesser extent, user studies. They are operational or execution risks, safety and hazard risks to human participants and risks due to leakage or breach of collected data. All three risk cases are thoroughly analyzed and whenever possible, we provide recommendations for implementation of risk mitigation procedures and industry best practices for safeguarding and proper handling of collected data.

1. Introduction

This report provides details of two kinds of experiments (robotic tests and user studies) planned as part of the work output of the Crowdbot project. Risks associated with both robotic tests and user studies are also assessed to better prepare and manage experiments to achieve desirable outcomes. This is the second in the series of a total of five reports that summarize key tasks in Work Package 1 (WP1). In the order of delivery/due dates, they are:

D1.1: Specification of scenarios requirements

D1.2: Experiment protocol and risk assessment

D1.3: Specification update

D1.4: Initial evaluation report

D1.5: Final evaluation report

Within WP1 there exists three project tasks:

T1.1: Scenarios Requirement

T1.2: User Studies Preparation

T1.3: Evaluation

Since there are three tasks and five deliverables, it is obvious that there is not a one-to-one match between a task and a deliverable but that one or more tasks in WP1 is responsible in generating each WP1 deliverable. To clarify the relationship between tasks and deliverable, we first review the timespans of each task (T1.1 to 1.3) and due dates of all five deliverables (D1.1—D1.5) in Figure 1.1. The illustration also provides a mapping of WP1 tasks responsible for each WP1 deliverable.

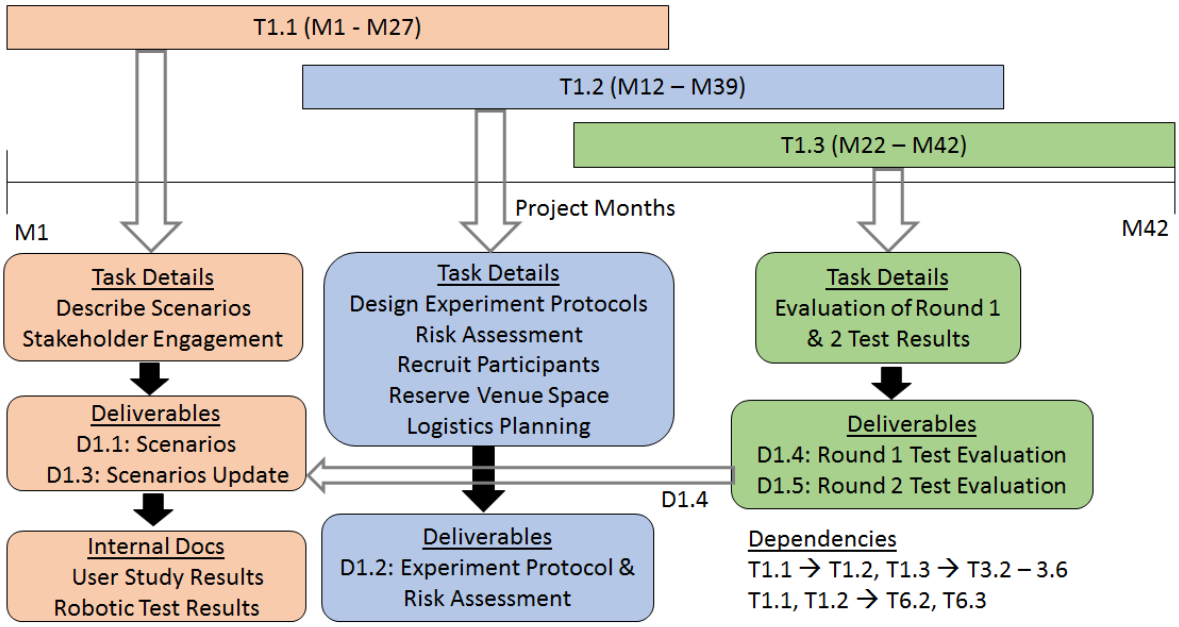

Figure 1.1: Work Package 1 tasks and deliverables

There are intra- and inter- Work Package dependencies. Deliverable D1.4: Round 1 Test Evaluation from T1.3 is used by T1.1 to prepare updated test scenarios in D1.3. In terms of Inter- Work Package dependencies, there are two: 1) T1.1, T1.2 and T1.3 are used to recommend certain specific technologies for Crowdbot robot navigation. The recommendations are based on initial proposed tested scenarios, revamped test scenarios based on round 1 test results, outcome from user studies and input from external experts and other stakeholders. 2) T1.1 and T1.2 will support robot design and ethics requirements of T6.2 and T6.3.

1.1 Stakeholders

A stakeholder is an external entity (a person, a group of persons, an organization, an enterprise or a government body) that is affiliated with the Crowdbot project. Seven categories are defined below to facilitate further discussions and their respective roles in support of the project.

1. **Users**: They are members of the general public that will directly interact with and use a service provided by a Crowdbot robot. The most obvious example is the human that sits and operates a smart wheelchair. A person that communicates with the Pepper humanoid (verbally or via its touchpad) is also a user. A customer that uses a service robot such of CuyBot for delivery or retrieval of stored items in this cargo space is also a user.
2. **Providers who care or assist such users**: These are professional and experts (commonly in the field of medicine, psychology and law) who are concerned about the ethics and well-being of robot users.
3. **Those who maintain or own infrastructure**: People in this category provide the physical space in which Crowdbot or similar type of robots may co-exist with humans in the future.
4. **Those in public service**: This category applies to staff members, agencies and government bodies that are responsible for maintaining law and order, rights and responsibilities and dispute resolution when accidents or entanglements occur among humans or between a robot and humans resulting from robot activity.
5. **Robot manufacturers or operators**: These are original equipment manufacturers (OEMs), robotic system integrators (SIs), resellers of robots and operators of robots. An operator is not necessarily a user but serves the role of an owner. For example, a smart wheelchair owned by a hospital is used by a patient. Likewise, a humanoid operated by an airport authority is used by airline customers and passengers.
6. **Outside experts**: These are technical and non-technical professionals with expertise in robotics, artificial intelligence, human crowd behavioral science, psychology, law, ethics and other disciplines related to Crowdbot project objectives.
7. **General public** (not part of the first six categories): They are people who do not directly interact with a robot but aware of its presence due to proximity or its (potential) existence via an information source (e.g. Crowdbot interview, online video or other media content, etc.) and are generally labeled as "by-standers."

As detailed in the next section (Sec. 1.2), the Crowdbot project will conduct two types of experiments: robotic tests and user studies. The former requires the participation of volunteers from the general public (category 7) while the latter provides a vehicle for Crowdbot team members to interact with several types of stakeholders. As we elaborate in Section 4, the focus of user studies is limited to "user group" stakeholders — specifically, categories 1 and 2. Recommendation and oversight of robotic tests in regards to safety and ethics are provided by outside experts (category 6) via the Ethics and Safety Advisory Board (ESAB), an external entity affiliated with the Crowdbot project.

1.2 Tests vs. Studies

The term "experiment" applies to two kinds of stakeholder engagements: robot tests and user studies. As noted earlier, two rounds of robotic tests are planned; each test involves a robot navigating among a dense human crowd environment. This implies robot-human interaction where both robot and humans are in motion. In contrast, user studies are sit-down interviews, networking sessions or similar activities between the Crowdbot team and stakeholders without the presence of a moving robot. Therefore, the protocol for a test event is quite different from that of a user study.

The remainder of this report is organized as follows: Sections 2 and 3 provide necessary background information and protocol details specific to a test event. Section 4 is exclusive to user studies. Sections 5 deals with Participant Recruitment which is applicable to both tests and user studies although the process is much more complicated for tests due to safety and ethical concerns stemming from robot-human interactions. Risk Assessment (pertaining mainly to tests) is detailed in Section 6. A large amount of data will be collected from both tests and user studies and a good subset of such data will be embedded with Personally Identifiable Information (PII). Section 8 provides a wealth of information of our data management process, policy and practices in safeguarding accumulated data during project period and beyond.

2. Test Venue & Resources

This section is specific to robot test events. Two rounds of test are planned during the project month intervals of M23-25 and M38-40. Each robot test involves a robot moving around humans in an open space or cluttered office-like environment. The system under test is composed of a mobile robot, human participants and a controlled physical environment. Specifics of a test event covered in this section are:

- Test sites: physical locations where robot tests will be conducted
- Material resources: equipment and objects required for successful execution of tests
- Logistics planning: reservation of test site, equipment and other resources

Details about the test event and its execution plan are provided in Section 3. Recruitment of human participants for test events is covered in Section 5. There exist two types of test sites: internal (partner) site and public (e.g. airport, train station) site. Initial proof-of-concept tests will be carried out at internal sites but it is foreseen that public sites will be used to validate and verify the efficacy of Crowdbot robots in crowded human environments. Below we first describe partner test sites, then followed by a description of potential candidates for public test sites.

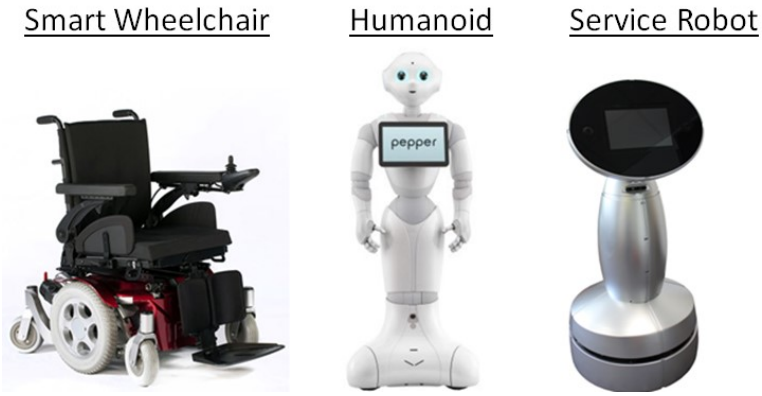

Figure 2.1: Crowdbot robots (Smart Wheelchair, Pepper Humanoid, Cuybot Service Robot)

2.1 Test Sites

A test site is defined as a physical address or name of the city of a partner's office or research laboratory facility. A test venue is a specific physical space (e.g. gymnasium, student center, robotics laboratory etc.) at a test site where the actual test event will take place. Among the seven partners of the Crowdbot project, three are robot owners. The smart wheelchair is developed by

UCL (London, UK), the Cuybot by Locomotec (Augsburg, Germany) and Pepper the humanoid by SoftBank Robotics Europe (Paris, France). The term "owner" refers to the partner that has the final discretion on how the robot is designed, sensors and processors are integrated and tested. Table 2.1 shows on-site availability of each Crowdbot robot.

Table 2.1: Crowdbot Robots & On-Site Availability

Robot	Owner	On-site Availability
Pepper Humanoid	SoftBank Robotics	SoftBank Robotics, Paris France
		INRIA, Rennes, France
		ETHZ, Zurich, Switzerland
Smart Wheelchair	UCL	UCL, London UK,
		INRIA, Rennes, France
CuyBot service robot	Locomotec	Augsburg, Germany

The lead for Work Package 3 (Navigation) is ETH Zurich and it is in charge of developing and integrating various navigation systems for Crowdbot robots. Thus, it is expected that both official (rounds 1 & 2) and internal test events will be held at its Zurich campus location.

It is anticipated that both test events (round 1 and round 2) will be conducted as different partner locations due to the availability of a test robot on-site and difficulty in transporting a robot from one partner location to another. Since the same Test & Evaluation team (led by INRIA and UCL) oversees all test events, it is expected that robot tests in each round will be carried out on non-overlapping dates. For example, for round 1 tests slated for the period M23-25, there will be three separate robot tests at three different test sites, spread over the three-month period.

For the smart wheelchair, the round 1 test will be conducted in an indoor and controlled environment—the PAMELA laboratory. It is a novel and highly flexible facility allowing full-scale pedestrian infrastructure to be built and tested to enable thorough assessment and evaluation. The structure includes a flexible floor surface that represents real ground conditions with interchangeable surface materials and is supported by a range of sensing equipment. More information can be found at https://www.ucl.ac.uk/transport-institute/lab/PAMELA

Round 2 test is expected to be conducted in a less controlled, open environment. It could be one or more of the following site.

Table 2.2: Round 2 Test Sites for the Smart Wheelchair

Location	Description
Aspire(Royal National Orthopedics Hospital)	The first leisure centre in Europe for disabled and non-disabled people. Located inside RNOH
Queen Elizabeth Olympic Park	It is a park located in east London. Free for entrance. Open environment.
UCL Here East Campus	The campus is based at Queen Elizabeth Olympic Park in East London

Figure 2.2 shows three good candidates that can serve well as public test sites. They are 1) hospital floor waiting area, 2) train station platform area and shopping venues and 3) airport terminal and duty-free shopping area. All three are carefully chosen due to their unique crowd behavior profiles.

The airport scene is always crowded but most people are wandering (not running) whereas at the train station, most are walking at a fast pace or running to catch the next train. In the hospital setting the environment is much quieter but the environment contains more clutter (e.g. furniture, hospital equipment). Each site is under the management of authority (e.g. hospital official, railway station operator, airport authority) and the team plans to engage with each authority in gaining necessary approval for conducting robotic tests at its facility.

Figure 2.2: Possible venues for public test sites

(a) University of Kansas Medical Center, Kansas City, Kansas, USA [1]

(b) Shinjuku train station, Tokyo, Japan [2]

(c) Heathrow airport terminal, London, UK [3]

2.2 Material Resources

Material resources can be further classified as venue objects, test equipment and auxiliary.

- *Venue Objects*: These are structural, mechanical or physical materials used for a test event at the venue space. Examples are furniture (tables, chair, etc.), office supplies (duct tape, whiteboard, pen and paper, etc.) and partitions and barriers (e.g. screens, pine cones, wood planks, etc.) and other items that constitute a test environment. In general, a test venue (a physical space) is modified into a test environment that mimics a real-world physical venue such as an office floor, hospital ward or a train platform etc.
- *Test Equipment*: These are typically electrical and electronic hardware devices and components used while conducting test events. Examples are lighting, electrical and computer cables, video and still image cameras for recording of test events, computer equipment for data logging and analysis, laboratory test and measurement devices, etc.
- *Auxiliary*: These are other material and resources that do not fall under the above two categories. Examples are office/laboratory space for pre-test planning and post-test data

analysis, automobiles or public transport options, food supply, lodging for visiting team members, etc.

2.3 Logistics Planning for Venue Space

For internal test sites, each partner is responsible for reserving venue space at its location. In general, there is padding of additional days (before and after test event day) to mitigate risks from bad weather, transportation disruption, electricity blackout and other similar triggers. For external public site reservations, the Program Management Office (PMO) will communicate directly with the venue owner or property manager to obtain proper ethics and operational clearances. Unlike internal test sites, no venue reservation is required for public sites such as train stations and airports since they are living and breathing spaces for public use.

2.4 Logistics Planning for Resources

As noted in Section 2.2, several types of material resources are needed for successful execution of each robotic test. Since tests are conducted are different sites (both internal and public), it is the responsibility of the test team to conduct an inventory check and plan ahead for acquiring and shipping of required material resources to the test site. There may be scarcity of certain material resources; hence, pooling of resources and time staggering of test events are recommended practices for risk mitigation. In general, the resource inventory list of each test event should track the following properties:

- Resource category and details
- Owner of resource and stored location
- Loaned location for test event
- Date of loan
- Expected return date to owner
- Shipping and tracking information of resource
- Team members and Point-of-Contacts responsible for loaning

3. Test Protocol

A test protocol consists of three phases:

1. Pre-test Planning
2. Test Day Execution
3. Post-Test Analysis

The pre-test planning phase includes preparation of test scenarios and test cases (Section 3.1), release of a test plan (Sec. 3.2) and formation of Test & Evaluation (T&E) team (Sec. 3.3). The test-day execution phase involves a pre-test safety check drill (Sec. 3.4) followed by execution of test cases. The order in which test cases are excluded is decided by the T&E team on the test day based on the availability of team members, material resources and other factors. At the conclusion of a test day, accumulated data is collected, securely stored and analyzed by the same T&E team. Further details of post-test data analysis is provided in Sec. 3.3.

3.1 Test Cases

Test cases are derived from test scenarios. A thorough description of test scenarios is presented in D1.1; here we provide a quick summary. There are seven main scenarios (labeled S1 to S7) defined for Crowdbot robot navigation tests. Each main scenario is then further classified into sub-scenarios such as S1.1, S1.2 and so on for the main scenario S1. Main scenarios S1 to S5 require human participation as a dynamic crowd whereas S6 and S7 are robot only tests. In D1.1 both main and sub scenarios are described at the system and operational levels without specifying minute details that are necessary to conduct a physical test event. On the other hand, test case is always based on a test scenario but with all minute details elaborated. For example, S1.1 refers to a simple one-dimensional flow scenario where a robot follows humans who are all traveling in a straight line in the same direction. To run S1.1 as a test case T1.1, we must also specify:

- The duration of the test and the number of repetition
- The speed at which both humans and the robot are moving
- The number of humans involved
- The position of the robot among the human crowd
- Safe personal buffer zone (distance between a human and the robot)

In summary, on the test day there will be a list of test cases (each labeled T x.y; x and y are positive integers); minute details of each test case is also well described in the test plan.

3.2 Test Plan

On the day of the test event, the Test & Evaluation team (see next section 3.3 for further details) will follow the test plan line-by-line. The test plan is a scripted instruction set of test cases that must or should be executed on each test day. Some test cases are marked as "required" or mandatory and others are marked as "optional" or supplementary. The T&E team check marks each test case that is executed. The test plan also records additional notes for each executed test case, for example, whether the execution is successful, issues and irregularities, if any. By the end of the day the T&E team evaluates the outcomes of the day's tests using the test plan and prepares a new test plan for the next day if the test event continues.

3.3 Test & Evaluation Team

The entire Crowdbot team is further grouped into sub-teams of Test & Evaluation (T&E), Technology Development (TD) and Robot Design & Quality Control (QC). These sub-teams are not mutually exclusive. A Crowdbot team member may belong to more than one sub-team; however, each sub-team is led by a different partner or partners. This division in role and authority allows the team to maintain a fair amount of independence among different sub-teams. The Test and Evaluation (T&E) team is in charge of the test plan, test execution and evaluation of test results. Details of the role and responsibility of the T&E team can be found in D1.1.

4. User Study Protocol

This section is specific to sit-down interviews and similar activities without the presence of moving robots. In general, user study will include structured interviews where participants are asked a fixed set of questions with their responses video/audio recorded. These recordings will be outsourced to an external company for transcription. The study will also have a focus group where participants have a discussion that is moderated by the researchers.

Figure 4.1 describes how user study fits into the whole picture of the project. It can be seen that T1.2 user study preparation is a prior for conducting user study of which result will be utilized for WP6-Recommendation for robot design and WP1 for test scenarios modification. Although there is no deliverable for the user study, it is essential as it reveals stakeholders' opinion which will affect ethical and technical considerations of this project.

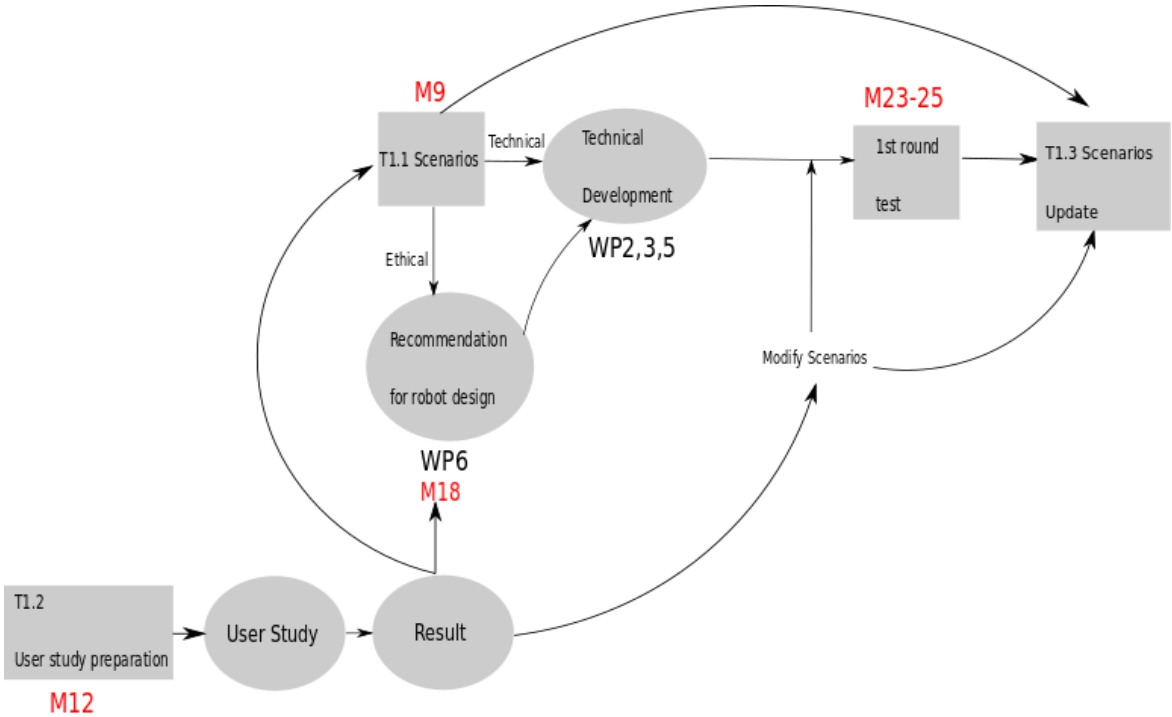

Figure 4.1: Relationship between user study and other work packages

4.1 Pre-Study Preparation

Prior to conducting the user study, preparation for participant recruitment, ethics approval and decision of questions is required.

4.1.1 Recruitment Campaign

Participants for the user study will be recruited from groups of stakeholders as discussed in Table 5.1. In order to recruit more people, a recruitment campaign will be kicked off in early January. Details is elaborated in section 5.

4.1.2 Ethics Approval

Ethics approval and data registration have been applied for to cover all legal and ethical aspects of the project as per UCL guidelines.

In terms of the ethics application, the research has been registered in the ethics database and an ethics application form has been to be submitted. All the personal and project details were included a 'low' risk application has been submitted for the REC Chair's review. All supporting documents such as Participant Information Sheets, Consent Forms and Recruitment emails were attached.

Following approval, any proposed changes, adverse events and report progress (if required) will be reported by the principal researcher on annual basis.

4.1.3 Deciding Questions

The value of the data collected from user study may largely depend on the effectiveness of the questions that are asked. Developing an effective list of questions is critical to the success of the user study outcomes

It should be noted that the choice of answers to the questions for structured interviews are often fixed, though open-ended questions can also be included. Besides, structured interview questions are usually kept in the same order as it is important to minimize the impact of context effects. Therefore, careful consideration of how to formulate the questions is essential. While developing questions for the interview, following types of questions should be avoided.

- Long questions and compound sentences that are difficult to parse.
- Leading questions that confirm what you want to know.
- Unconscious biased questions.Different from the structured interview, questions for focus group are more open-ended. In general, following three types of questions will be used.
- Engagement questions – Introduce the participants to the topic or subject and get them comfortable with the discussion.
- Exploration questions – Designed to get to the heart of the discussion and typically are open-ended.
- Exit questions – Designed to see if any angle was missed during the discussion.

In this project, specific questions for structured interviews and focus groups studies will be prepared based on the objectives of the study and the way its outcome relates to other work packages.

As shown in Figure 4.1, the outcome of the study relates to WP6 for EPFL to develop recommendation for robot design which will further affect the technical development. Therefore, it is crucial to understand stakeholder's level of acceptance for certain test scenarios to avoid ethical issues. In general, questions should cover two aspects: crowds and robot.

As this user study will be conducted for three robots, the similarity and difference of these robots should be taken into account. For example, social navigation scenario is only considered for Pepper, which is expected to show naturalness and sociability in addition to safety and comfort.

In order to increase the efficiency of the user study, a list of questions will be prepared for each CROWDBOT partner asking their specific requirement/region of interests/anticipation for this user study. Based on which, questions for structured interviews and group studies will be designed and target participants will be recruited.

4.2 User Study Tools

The stakeholder engagement will utilize the following tools:

1. Recorder--Interviews will be digitally recorded.
2. Notebook, worksheet and post-it notes—Notes will be taken and collected for focus group study.

4.3 User Study Plan & Execution

Table 4.1: General User Study Plan

Activity	Time
Structured interviews	Feb-March 2019
Focus group engagements	March-April 2019

General plan for the user study:

1. Interviews: These will occur in a public location agreed upon with each participant. Prior to the study, participant information sheet will be distributed and the participant needs to sign a consent form. The interview will be semi-structured, digitally recorded, transcribed and then analyzed using thematic analysis (Braun & Clarke). Each participant will be asked exactly the same questions for consistency. It is expected to last, at most, 60 minutes.
2. Focus groups: These will be organized at Here East and will take a mix of stakeholders as shown in Table 5.1. On the day of the focus group study, participant will be received at the entrance of the building and the study is likely to happen in a meeting room. Prior to the study, participant information sheet will be distributed and the participant needs to sign a consent form.

   Participants will be divide into groups of 6-8 people and a facilitator will lead a discussion. Notes will be taken by a scribe and also collected using a worksheet and post-it notes. The focus groups will cover the following aspects:

   a. Where do people most encounter crowds?
   b. Are some crowds better than others?
   c. How do people feel when in a crowd?
   d. What are the constraints on managing crowds in buildings?

   The second half of the focus groups will have specific stakeholder groups grouped together. Here each stakeholder group will look at specific aspects of navigating in crowds/controlling crowds/safety etc. Focus group will take about 60-90 minutes.

The user study will be considered as a success if the research question is answered and acceptance is obtained. However, failure may occur if respondent does not provide usable material. This could happen if the participant feels annoyed or become skeptical. Remedy for these situations could be, appropriate pause, rephrase the question or reschedule another appointment.

5. Participant Recruitment

This section applies to both tests and user studies although specifics and target participants may differ.

5.1 Recruitment Process

The process of recruitment will take the form of building a community of practice around the project, with a kick-off stakeholder engagement day where we will invite people from the stakeholder groups listed in Table 5.1. This may vary based on other partner's needs for the user study.

Table 5.1: Stakeholder Groups and Local Contacts

Stakeholder Group	Local Contacts
Electric wheelchair users	ASPIRE; Whizzkidz; QEF;
Facility/Space managers	Queen Elizabeth Olympic Park; Olympic Stadium; Transport for London (TfL); Dept. of Transport
Medical Practitioners	RNOH(Royal National Orthopedics Hospital)
Wheelchair Manufacturers	Quickie Wheelchair
Assistive Technology Expert	UCL, RNOH
Public	Built Environment Access Panel (BEAP)
Others	

Recruitment channels can be forums, social media, emails and so on. In order to recruit enough participant for the user study, a technique called snowball sampling can be used. It often starts by asking people you want to interview who are likely to know others like themselves for referrals. Then the referrals can provide still further referrals.

Recruitment process usually takes a couple of months. The engagement plan is listed in Table 5.2.

Table 5.2: Brief Engagement Plan for Participant Recruitment

Activity	Date
Plan the launch/kick off day	Dec 2018
Identify individuals	Dec 2018
Send invitations	Jan 2019
Book room/refreshments etc	Jan 2019

It should be noted that normally a 50% dropout rate should be expected. Therefore, people been recruited should always exceeds the actual required number of participants. If some participants didn't show up, we could contact them for confirmation if contact information is provided. Otherwise, in terms of focus group study, it should be continued as it is unfair to cancel or reschedule for the people who turned up. As for interviews, it is easier to reschedule.

5.2 Participant Rights & Responsibilities

Privacy issue and protection of personal data: In terms of the study 'Scenario requirements for safe robot navigation in dense crowds', participants have certain rights under data protection legislation in relation to the personal information that we hold about you. These rights apply only in particular circumstances and are subject to certain exemptions such as public interest (for example the prevention of crime). They include:

- The right to access your personal information;
- The right to rectification of your personal information;
- The right to erasure of your personal data;
- The right to restrict or object to the processing of your personal data;
- The right to object to the use of your data for direct marketing purposes;
- The right to data portability;

To ensure privacy, all information collected from participants during the study will be kept strictly confidential. All the data will be anonymised so that participants are not identifiable in any ensuing reports or publications.

The data controller for this project will be University College London (UCL). The UCL Data Protection Office provides oversight of UCL activities involving the processing of personal data, and can be contacted at data-protection@ucl.ac.uk. UCL's Data Protection Officer can also be contacted at data-protection@ucl.ac.uk**.**

Further information on how UCL uses participant information can be found at [4].

Compensation for food and travel expense: Reasonable travel expenses will be reimbursed for all structured interviews and focus group studies based on receipts. Refreshments will be provided.

Each participant's role during a user study event: Participants will be interviewed and/or participate in one or more focus group study.

Data Collection and Release: The data collected during this research study will be used for dissemination (publication in articles, presented within a PhD thesis), and to identify scenarios in which robots can operate within crowds of people. All information collected from participants during the study will be kept strictly confidential. The data will also be anonymised so that participants are not identifiable in any ensuing reports or publications. All data will be stored on an encrypted drive that is accessible only to project members. No PII data will be released to public. For structured interviews, an external agency will be used to transcribe the data. No other use will be made of the data without prior written consent from the participant involved.

Notice will be made to participants if the processed data is released and copies of the publications could be distributed to the participants based on their interests.

Legal action due to misuse: If data is misused, UCL is obligated to notify the national data protection authorities of data breach without undue delay and additionally notify the individual if there is a high risk that rights and freedoms are violated.

Formal complaints resulting from participation in this study should be lodged with the Principal Investigators, Dr Catherine Holloway c.holloway@ucl.ac.uk

Should the participants feel their complaints have not been handled to your satisfaction, contact the UCL Research Ethics Committee – ethics@ucl.ac.uk

Participants can also complain to the Information Commissioner's Office (ICO) about the use of their personal data.

Right to negate participation pledge or leave during a test: This is a voluntary study and participants will be given consent forms to sign if they decide to take part. According to GDPR, Participants have the right to withdraw such consent at any time, which means participants are allowed to leave during the study without providing a reason at which point they will be asked what they wish to happen to the data they provided up to that point. Reasonable travel expenses will still be reimbursed if the participant leave during the study.

6. Risk Assessment

This section applies mainly to tests. There are risks associated with user studies such as no-show by participants and slippage in study completion date but they are considered minor compared to risks associated with robotic tests. There are two types of risks for robotic tests: safety (for human participants) and project (for meeting goals and objectives). We assess risks associated with each case below. We also provide recommendations and best-practice guidelines to mitigate or reduce the possibility of such risks arising during test events. The last section 6.3 addresses the topic of data management. Both user studies and robotic tests will generate a wealth of data that must be collected, stored, transferred, processed and in some cases, released to parties outside of the team. We evaluate risks associated with the handling of such data and recommend best practices (access control and encryption) that should be implemented to maintain ethics and integrity of the team and project as a whole.

6.1 Safety: Risk Due to Injury & Bodily Harm

Crowdbot robotic tests require movement by both human participants and a robot under test. Motion speeds are typically at the pedestrian stroll level; however, contact and possibly collision between humans and the robot may not be avoidable. There is also a high chance of human-to-human or human-object collision due to avoidance of the robot by humans. Furthermore, weight and material composition is different for each Crowdbot robot. The heaviest robot, the smart wheelchair, has protruding front caster wheels and a metal footrest that can easily cause bodily harm even at a low speed of collision. Since a human sits on the wheelchair while it is in motion, the total gross weight of the wheelchair can be in excess of 200 kg. The smallest and lightest Crowdbot robot is the humanoid Pepper. Its frame and weight are similar to that of a small child and the outer material is mostly plastic. In this case there is less concern of bodily harm when colliding with Pepper but the possibility of Pepper tipping and falling is high due to its small form factor and light weight. A Pepper fall may cause humans to react reflexively and thus cause human-human contact or injury. If Pepper falls on a hard surface, it body frame may decompose and cause internal parts to shatter.

To reduce the possibility of such risk occurrence, it is assumed that the Crowdbot test team will provide dos-and-don’ts safety procedures and risk mitigation plans before the commencement of each robotic test. Furthermore, it is expected that the team has in place medical first-aid kits and emergency protocols in case a human participant becomes sick or injured at the test site.

6.2 Project: Test Execution & Completion Risk

Various scenarios are possible for poor or incomplete execution of a test event. Below we list the main concerns:

1. *Lack or Malfunction of Robot*: A test event is of no value without the presence of the robot under test that is operating as designed. This requires all its technology features (sensors, processors, software and locomotion) to be functioning in-sync. Any malfunction would result in a modified test plan where certain test cases are omitted or modified in scope. On a different matter, the absence of a robot on test day would void completion of any test cases but that likelihood is low since the robot is assumed to be present at the test site a few days before the test day for preliminary checks and rehearsals.
2. *Deficiency in Test & Evaluation Team*: The team is composed of persons of various skill sets for robot operation, data collection, test case execution and so on. If the team composition is well-designed such that each member is assigned primary as well as secondary roles (in case of an absence by another team member), a test event failure due to absence of team member(s) can be avoided.
3. *Deficiency in Human Participants*: A majority of Crowdbot robotic tests require the participation of human crowds. In general, a crowd size more than 30 is required to conduct a successful test since most tests involve a moving robot and a dense crowd must be maintained around its immediate vicinity as the robot traverses a path. Experience has shown that the no-show rate of committed participants is around 50%, and sometimes as high as 80% due to weather and other external conditions. Three mitigation strategies are foreseen: 1) Excess Recruiting: This is a simple strategy with a number of drawbacks. If more participants than required are present at the test event, the team may have to send home some of them and find an option for all to participate. Over-recruiting is also costly since the team must pay for their travel and associated expenses. 2) Test events are conducted over multiple days. This strategy has clear technical and operational benefits compared to option 1 at the expense of logistical costs and expenses associated with running a test event over multiple days. 3) Use of team members as participants an elastic strategy to increase participant count.
4. *Lack or Deficiency in Venue Space*: No venue equals no test event. The possibility of such an outcome can be reduced by reserving a venue by padding additional days. Furthermore, the team should devise a backup plan if the venue of choice is not available. An alternate site must be considered in advance if the first option fails. Another related issue is that the venue is available but its space and structure is not suitable for certain test cases. In this case, the test plan is revised or the venue space is modified to accommodate the requirements of certain test cases. The test team must anticipate and prepare for such scenarios in advance.
5. *Lack or Deficiency in Resources*: A number of material resources (big and small) are critical for successful execution of a test event. The lack or malfunction of a computer cable, an electronic sensor or a battery charger device may change the outcome of a test case. However, it is expected that most critical items required for a test event will be identified in advance, their availability logged and confirmed and if necessary, backup options are

considered. In certain cases, two or more identical sets of resources are available to the team. It is expected that such risk mitigation procedures are implemented by the test team.

6.3 Data Management

This section pertains to both tests and user studies. Both collected and generated data are covered. Data management procedures for the Crowdbot project are detailed in D8.2: Data Management document, which is an official deliverable to the European Commission but it is released to the public. Here, our focus is to address data management as part of risk management. That is, we cover issues associated with collecting, storing, transferring and releasing of data pertaining to user studies and robotic tests.

6.3.1 Data Collection

It is expected that both analog (e.g. paper, hard copy) and digital (electronically signed documents, image and video files, electronic data sets) will be collected during both user studies and test events. Paper documents such as participant consent forms and personal contact information sheets may exist in the original analog format or converted to its equivalent digital format via scanning or camera imaging. All collected analog material must be physically secured (e.g. storage in a locked cabinet or drawer) or if converted to its digital form, it must be properly disposed via shredding and safe discarding.

All collected digital material must be secured properly. Both physical and electronic security measures must be used as appropriate. During the day of user study or test event, those in charge of the experiment must clearly state who is in charge of data collection, the type of resources used for data collection (binders for collected paper, hard drives and USB sticks for electronic data, etc.) and logging of the status of collected data by the end of the experiment. For example, the data collector must record the number of paper sheets collected, the amount (in terms of data bytes) of electronic data collected, and who else, in addition to the data collector, has gained access to the data. In certain experiments there may be more than one data collector and thus the data collection log must be representative of all data collected.

6.3.2 Data Storage & Transfer

After the data collection phase, risks associated with data storage and transfer must be addressed. Data storage refers to permanent retention of collected data until destroyed or discarded. We have already addressed risks associated with analog data and appropriate means for safeguarding of such data. In this section our focus is digital data storage. Collected digital data for user studies and test events are broad. Here we name a few: correspondence data of participants (personal information such as name, age, address, e-mail account or telephone number, etc.), test/study data (venue, time/date, video, audio, sensor data, user responses to questions, etc.) and project data (any data outside of the first two such as budget, travel expenses and itineraries). All three categories of collected data is likely to be embedded with Personally Identifiable Information (PII) and/or Project Sensitive (proprietary, non-public) information. Hence, care must be taken and proper procedures must be followed for both storage and transfer of such data. Collected data can be stored internally (on the storage of the electronic device or computer used to collected such

data), externally (on an externally connected hard disk drive or some other non-volatile memory unit) or remotely (such as storage unit at a data center).

First, we examine risks associated with all three types of data storage options. Internal storage such as the hard disk drive of a computer has some safeguards against intrusion and unauthorized release but its weaknesses must also be known to the collector. Most computers have access control (user id and password check) but this does not directly protect data content stored on the disk drive. Some institutional and enterprise computers use automatic backup of hard disk data such that collected data may be copied and stored at a remote location without knowledge by the collector. Another risk is administrator rights by a third party to access stored data on a computer by some authority in person or remotely. Thus, the collector must be aware that the only means of securing stored data is via encryption. Many commercially available strong encryption solutions exist for protection of Crowdbot collected data. Certain electronic devices such as cameras and smartphones store data on internal or removable storage media. In almost all cases such stored data is not encrypted and access to such data is not protected. A loss of the electronic device or its storage medium constitutes a data leak. The same applies to external storage media such as USB thumb drives and external hard disk drives. Unless protected via both access control and data encryption, the collected data is at risk from tampering and leakage.

Remote storage of collected data poses additional risks. Third-party storage offered via online cloud services is convenient for sharing among team members due to its remote access capability. This, however, comes at a cost. The storage medium itself is owned by a third party and in some cases, not by the cloud service provider. The stored data can also be replicated or segmented fat multiple physical locations for convenience, on-time availability and efficiency. It is important to note that with proper data protection procedures (access control and data encryption) in place, remote storage is a safe and efficient option for both collected data storage and transfer.

Copying of collected data from one storage medium to another is considered a data transfer. Examples of transfer from internal storage to external hard disk, internal storage to remote storage, external hard drive to remote storage or embedment/attachment of data in electronic message exchange such as e-mail or file transfer. In all these cases the associated risk is leakage. For example, when transferred from an internal hard drive to an external unit, the latter may not have proper access control or built-in encryption. If the external storage unit is lost or tampered with, embedded data may have leaked. Likewise, when data is transferred remotely via cloud service or e-mail exchange, copies of such data are replicated and/or stored at locations that may not be protected. Therefore, it is strongly recommended that any data transfer includes restricted access control and data encryption features.

6.3.3 Data Release

Data release applies to any collected data that is published, shared with a third party, uploaded to a publically accessible location or leaked. Let us assess the risks associated with each scenario. When data is published as analog hard copy or digital online content, it is accessible by the general public, hence, it is released to the public. When data is shared with a third party (i.e. any non-public entity), there is possibility of subsequent release to outside parties or even to the public. Uploading

of data to a publically accessible location such as a website, cloud storage server or attachment in an e-mail exchange may result in data leakage even if the website, cloud service and e-mail exchange services are access controlled. This is because the networks and systems that maintain such services may be vulnerable to attacks and intrusion or passwords used to access such services are compromised. Another possible source of data leaks is due to loss or theft of storage devices. In all these cases data may or may not be released to the public but once data leaks occur, it is very difficult to trace the leak route; that is, we may never know who has access to the leaked data.

There is no legal or ethical concern if released data has already been cleared for public consumption, reprint and further dissemination. However, if data is not approved for public release, any of the release scenarios stated above may violate European, national and individual privacy laws. This raises another concern for the release of collected data: What checks and balances are in place before release? Here, two separate types of risks must be assessed. First, all team members in possession of collected data must have clear knowledge and understanding of whether each data item is releasable or not. Here. The term "releasable" applies to sharing of collected data with a non-Crowdbot team entity, and not necessarily the general public. The team cannot share collected data with an external entity but simply stating "This is non-public data; please treat it carefully." This is a sticky issue that many large commercial Internet Technology companies have exploited by stating: "Your information is private, not public but maybe shared internally or with our affiliates." When a data leak results from a secondary recipient, the original owner claims no violation of its data privacy policy since it is not the source of data leak. Second, all team members in possession of collected data must be aware of various mechanisms listed above where data is released or leaked unintentionally because proper safeguarding measures were not practiced. Such risks are fairly high since most projects do not train their team members in proper handling of data.

Finally, we consider the remaining issue: What happens to data that is not released? Any data not released is either retained, destroyed or discarded. Retention applies to any data that the team has explicit knowledge of possession and decides to maintain a copy for future use. When data is destroyed, the action is carried out with explicit knowledge that the reverse process of recovery is no longer possible. Various destruction methods exist such as shredding or burning of analog paper, electronic deletion of digital data, complete wipeout of storage medium or even physical destruction of the medium. Data is discarded when its status is no longer tracked. The team is no longer concerned about its state (e.g. where it is stored, who has access, how large the byte size and specific details of its contents) or have forgotten or misplaced it. The most prevalent scenario of discarded data is when a team member stores collected data on an electronic device, computer or remotely on a cloud storage and then leaves the project, hired institution or simply loses track of its state. Data leak from discarded data is very high. Protection of stored data by applying strong encryption is recommended to lessen such kind of data leak.

In general, all data (both publically releasable and private) should be encrypted. Encryption passwords and keys should not be reused when securing different data sets. Thus, a key management procedure must be agreed upon among all team members and diligently followed by all without deviation. That is, once a data set is encrypted, it must be decrypted and then re-encrypted with a different key or password. All decrypted data set must be destroyed, deleted or re-encrypted with the same key or password.

References

[1] https://www.bdcnetwork.com/new-medical-office-building-7-things-know-about-today%E2%80%99s-outpatient-clinic; photo courtesy of Gayle Babcock, Architectural ImageWorks, LLC.

[2] https://www.shinjukustation.com/shinjuku-station-building-facilities/

[3] https://www.ibtimes.co.uk/heathrow-airport-nigerian-travellers-are-biggest-spenders-vip-services-luxury-goods-1491470#slideshow/1428277

[4] www.ucl.ac.uk/legal-services/privacy/participants-health-and-care-research-privacy-notice