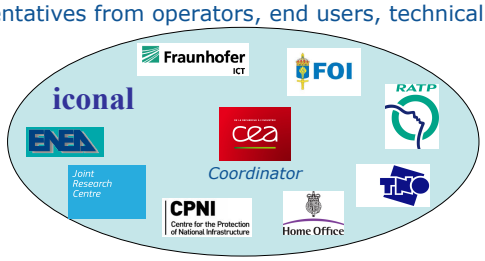
Detection of Explosives Materials for Operational Needs (DEMON)

P. Charrue, D. Poullain
CEA

What is DEMON?

- Thematic group of ERN CIP project
- Gathers representatives from operators, end users, technical experts



ratp

- Why DEMON?
  - Since 2006, EU and DG MOVE have defined legally binding technical specifications and performance requirement standards for various types of detection equipment used within EU airports.
  - Development of an European Common Testing Methodologies (CTMs) for detection equipment, in view of facilitating mutual recognition of approved or certified equipment. This activity is developed by the European Civil Aviation Conference (ECAC).

This kind of organisation is not yet in place for the detection of explosives outside the framework of aviation security

What is DEMON?

Objectives

- Provide support on technical specifications and detection requirements for the different configurations identified as typically significant for the field;
- Assess/suggest conformity testing methodologies based on the technical background of ERNCIP-DEMON members;
- Provide support on the conception and design of an EU accreditation and certification system;
- Provide support on trialling activities;

Strategy action

- Compilation of operational needs for explosive detection outside aviation security area
- Technical requirements to reach these needs
- First elements of a European CTM outside aviation security area

Needs

Goal: identification of user needs in the area of explosives detection for infrastructure protection applications

Means: internal working meetings, feed-back from events (OG 2012), operators views (RATP), meeting with DG MOVE (maritime)

Definition of infrastructure: any building, site, event, etc., warranting protection from explosives-based attacks.

Needs

4 infrastructures categories

- Specific site with a secure perimeter, and low-to-moderate entry/exit throughputs (e.g. secure government or commercial office building, civil nuclear site)

- Specific site with a secure perimeter, and high or very high entry/exit throughputs (e.g. sports stadia, concert arenas, music festivals, major event venues, major museums, ports

- Specific but open site, moderate to very high volumes of people (E.g. shopping centres, main railway station concourses, land-side public areas at airports

- Complex network, moderate to very high volumes of people (E.g. mass transit system)

Needs

Considerations of needs by infrastructure

Comments on:

- screening measures and process: time for screening, flow, level of explosive threat, permanent or not, screening needs (people, luggage, vehicles,…)
- complementary security measures: secure perimeter, personnel security measures,…
- process needs: space, manual search or/and technologies
- equipment needs
- staff needs: training, number, permanent or occasional,…
- opportunities for improving capability: technologies, design, alternative approach to technologies,…

Needs: example

Complex network, moderate to very high volumes of people (e.g. mass transit system)

- Multi pedestrian entrances
- Operate daily and sometimes 24/24
- Pedestrian flow varies from moderate to very high
- Screening measure which delays people is unacceptable (not possible to require people to divest)
- No screening of vehicles or deliveries
- More impactful search may be tolerable for short period

Screening options:

- screening people and their possessions as they enter the network (ticket barrier). Resolution of alarms will be highly challenging given the flow rates. Costly (but would maximize assurance) if applied at all points of entry.
- screening people as they travel around the network: would provide limited assurance as only a proportion of people would be screened.
- permanently and automated installed measures could be completed by randomly highly visible solutions (deterrence) (walk through metal detectors, dogs, manual search,…)

Needs: example

Complex network, moderate to very high volumes of people (e.g. mass transit system)

Process needs

- screening of high volumes of people, cost effectively, no need to divest and no delay for people
- need to be accepted by public and not privacy invading

Equipment needs

- technologies for high throughput, non contact screening of people and their possessions than can be integrated into existing infrastructures
- Low cost and compatible with environment (dust, humidity, vibrations,…)
- Low false alarm rate

CONCLUSION AND FURTHER WORK TO ENGAGE

- Each of the four infrastructure categories have to be deeply examined in order to detail specificities and challenges to overcome in detection (work which could lean on the GAP analysis results already implemented by DG/HOME in the frame of MATRIX group and NDE),

- Corresponding scenarios of attack must be defined and approved by EC,

- Detection devices which could be used for each category should have to be certified at National and EC level according to specific CTM defined for the considered application

- To engage the process we could suggest to take a very well defined configuration (e.g. checking of ferries on harbors) and develop all the different steps from the state of art till the implementation of a dedicated European Agency which could be similar to the ECAC for aviation security