[PRACTICE]

D5.5 SAFE ROOM DESIGN

PRACTICE WP5 deliverable

Dissemination level: Public

Nature: Deliverable

UNCLASSIFIED

SEVENTH FRAMEWORK PROGRAMME

PREPAREDNESS AND RESILIENCE AGAINST CBRN TERRORISM USING INTEGRATED CONCEPTS AND EQUIPMENT

practice.fp7security.eu

UNCLASSIFIED

Title:	D5.5 Safe Room Design	
Date:	October 24, 2012	
Author(s):	N Hale, D Kelly	CBRNE Ltd

This project has received funding from the European Community's Seventh Framework Programme. The views expressed in this document are purely those of the writer and may not in any circumstances be regarded as stating an official position of the European Community.

Summary Work Package 5

The overall aim of the project “Preparedness and Resilience Against CBRN Terrorism using Integrated Concepts and Equipment” (PRACTICE) is to improve the ability to respond to and recover from a Chemical (C), Biological (B), Radiological (R) or Nuclear (N) incident. The objective of the project is to create an integrated European approach to a CBRN crisis – i.e. a European Integrated CBRN Response System. This will be achieved through the development of an improved system of tools, methods and procedures that is going to provide EU with a capability to carry out a truly integrated and coordinated operational reaction following the occurrence of a CBRN crisis, whether it is caused by a terrorist act or an accident.

The objectives of WP5 are to develop, integrate and test a complete toolbox for first responders, decision makers and the public, including innovative components developed during the project to provide an improved and integrated preparedness and response to CBRN events.

The tools will be organized in 6 categories:

1. Recommendations
2. Standards
3. Protocols / procedures
4. Equipment and systems (eventually simulated): hardware, software, with performances, Technology Readiness Levels (TRLs), validation/certification status
5. Simulated environment (with 3D databases)
6. Real equipment and system emulation capabilities.

These tools will fulfil functions as defined in WP3, organized in line with the ESRAB/Staccato taxonomy functions, completed and detailed when needed for PRACTICE. The toolbox should be considered as living system gathering “bricks” into an integrated solution to manage a CBRN crisis. It will include actual tools and equipment and ICT simulated environments including hardware and software. This will allow plugging and playing new components and guarantee their interoperability.

The toolbox will be developed and integrated in two steps:

- A V0 version integrating in an innovative way existing validated capabilities (fed from WP 2 and WP 3) i.e., tools, methods and procedures that will be put together into an information system, with specified standard interfaces.
- A V1 version integrating innovative tools, methods and procedures and supporting future standards to improve interoperability and consistency without impeding the existing operational systems.

Developing V0 and new CBR tools for V1 will be an iterative process with all the stakeholders in the loop. Focus will be put on specifying simple interfaces for any supplier to describe and present its "bricks" in order to "index / reference" them in our PRACTICE Toolbox Information System. Any new tool that satisfies the "standards" interfaces should be easily added to build new solutions ("buildings").

Work Package team:

Frédéric Perlant	Astrium S.A.S. (AST)
Wilfrid Lefebvre	Astrium S.A.S. (AST)
Erik Bakke	Bruhn Newtech A/S (BNT)
Stéphanie Damiot	Cassidian S.A.S. (EADS)
Dominic Kelly	CBRNE Ltd (CBRNE Ltd)
Nigel Hale	CBRNE Ltd (CBRNE Ltd)
Jamie Braybook	CBRNE Ltd (CBRNE Ltd)
Kristian Krieger	King's College London (KCL)
Athanasios Sfetsos	National Center for Scientific Research "Demokritos" (NCSRD)
Frank van het Veld	Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
Ingrid Bastings	Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
Ed van Zalen	Netherlands Forensic Institute (NFI)
Kristi Mo	Norwegian Defense Research Establishment (FFI)
Iain Clark	Selex Galileo Ltd (SELEX)
Giuseppe La Posta	Selex Sistemi Integrati SPA (SSI)
Josef Brinek	Statni Ustav Jaderne, Chemicke A Biologicke Ochrany vvi (SUJCHBO)
Ola Claesson	Totalforsvarets Forskningsinstitut (FOI)
Paul Hooijmans	Prometech BV (PRO)
Florian Käding	Prometech BV (PRO)
Luc Sengers	Prometech BV (PRO)
Pierre-Alain Fonteyne	Universite Catholique de Louvain (UCL)

Glossary of Acronyms

CBRN	Chemical, Biological, Radiological, Nuclear
CCTV	Closed Circuit Television
COLPRO	Collective Protection
CPNI	Centre for the Protection of National Infrastructure (UK)
DNA	Deoxyribonucleic acid
EU	European Union
FEMA	Federal Emergency Management Agency (USA)
FP7	Framework Programme 7
HEPA	High Efficiency Particulate Air (Filters)
IMCOSEC	IMprove the supply chain for COntainer transport and integrated SECurity simultaneously
PRACTICE	Preparedness and Resilience Against CBRN Terrorism using Integrated Concepts and Equipment
TEDA	Triethylenediamine
TRL	Technology Readiness Levels
TV	Television
WC	Water Closet
WiFi	Wireless Fidelity
WP	Work Package (of Project PRACTICE)

Contents

1. Executive Summary

This report provides guidance in the specification of Safe Rooms designed as a response to the threat to people from Chemical, Biological or Radiological (CBR) incidents. It does not provide guidance in respect of protection from energetic missiles or explosives. The document is to be considered as a route map for those interested in developing their own Safe Room, not detailed design advice. It provides sufficient detail such that an interested party (e.g. a school, office or factory) can understand the key design parameters that they will need to specify to a detailed design specialist. It also provides a stepwise process (to be undertaken with the help of expert parties e.g. security experts, architects etc) to the development of a detailed specification that can be handed-on to other expert parties to develop the detailed solution. Its use will thus ensure that the user is an "intelligent customer" who procures what is needed rather than what is simply available or offered.

The report examines the key functional requirements to be addressed when designing a Safe Room: these are identified as Isolation, Sustenance, Access and Communications.

Issues to be considered in providing these functional requirements are examined and best practice guidance is presented. Finally a design selection process for Safe Rooms is presented which is driven by an assessment of Design Basis Threat[1]. For non-technical users of Safe Rooms this is considered to be preferable to the simple purchase and installation of off-the-shelf products or products designed to one of the established "classes" such as those defined by the Federal Emergency Management Agency in FEMA 452 for example.

Consideration of the issues associated with the activation of a Safe Room by commercial organisations (rather than military organisations for example) has led to the conclusion that the benefits from inclusion of decontamination and monitoring facilities in a Safe Room are likely to be outweighed by the difficulties in their operation. Furthermore, if such facilities are required prior to allowing personnel into the Safe Room then it is likely that it is already too late to use them. Thus Safe Rooms – as set out in this report – are proposed as part of a planned response to a raised threat or a response to an imminent threat rather than a response to an incident which has already caused personnel contamination. Decontamination facilities are therefore not addressed in this document.

This document can be used in two ways; users can either read through the guidance presented in Sections 3 to 6 and then use the flowcharts in Section 7 to help them generate a specification (this

[1] A "Design Basis" threat is a defined threat or scenario, which encapsulates the scope of threat that is to be designed for – i.e. anything worse than the design basis threat is to considered to be beyond the scope and by definition does not need to be explicitly addressed. The reasons for choosing this boundary can, for example, be based on risk, cost, finance or political factors. It is a concept commonly used in high risk industries (see IAEA).