CREATIF

Network of Testing Facilities for CBRNE detection equipment

Deliverable Report D.3.1

Operational Testing Framework

Peter Myers, Pär Wästerby, Friederike Strebl, Jasper Kieboom

May 2010

CLASSIFICATION LEVEL: PUBLIC

SEVENTH FRAMEWORK PROGRAMME

CREATIF is an FP7-funded project

Contract No. 217922

Table of contents

Deliverable Report D.3.1 ... 1
Table of contents ... 2
1 Executive Summary ... 5
2 Introduction ... 8
2.1 Objectives to perform operational testing ... 8
2.2 Principles of CBRNE detection ... 10
2.3 Specifics of chemical detection ... 11
2.3.1 Typical agents ... 12
2.3.2 TIC's and TIM's ... 13
2.3.3 Simulants, test agents and interferents ... 14
2.4 Specifics of biological detection ... 14
2.4.1 Typical agents ... 16
2.4.2 Simulants and interferents ... 19
2.5 Specifics of radiological/nuclear detection ... 20
2.5.1 Typical technologies used by these types of detectors ... 21
2.5.2 Maturity of the technology for field use (application for field use) ... 23
2.5.3 Typical agents (to be used in a "dirty-bomb" scenario) ... 23
2.5.4 Simulants and interferents ... 24
2.5.5 Interference testing ... 25
2.6 Specifics of explosive detection ... 26
2.6.1 Typical explosive agents ... 32
2.6.2 Interference testing ... 33
3 Operational testing – the concept ... 35
3.1 Introduction to the elements of operational testing ... 37
3.2 Scenario based operational testing ... 38
3.2.1 Selected chemical scenarios for operational testing ... 38
3.2.2 Selected biological scenarios for operational testing ... 40
3.2.3 Selected radiological/nuclear scenarios for operational testing ... 42
3.2.4 Selected explosive scenarios for operational testing ... 42
3.3 Introduction to human factors testing and evaluation ... 45
3.3.1 Historical background ... 45
3.3.2 Application to CBRNE detection equipment testing ... 46
3.3.3 Human factors testing and evaluation – A starting point ... 46
3.3.4 Human factors testing example ... 48
3.4 Test and evaluation of performance in an operational environment with human factor considerations ... 52
3.4.1 General performance testing ... 52
3.4.2 Detector Usability ... 52
3.4.3 Evaluation of the user's manual ... 54
3.4.4 Operational interaction ... 55
3.4.5 Throughput testing ... 56
3.4.6 Personal protective equipment in operational testing ... 56

3.4.7 Inclusion of decontamination testing within operational testing 58
3.4.8 Costs of operations 59
4 Evaluation protocols – Performance metrics... 60
4.1 Introduction.. 60
4.2 Rating schemes.. 60
4.3 Rating levels 63
4.4 Maintenance of the rating scheme and rating levels 64
5 Reporting guidelines 65
5.1 Introduction.. 65
5.2 Suggested reporting format 65
5.3 Characteristics tables 66
6 Other considerations.. 71
6.1 Cost/benefit for operational testing and standardization 71
6.1.1 Cost of testing 71
6.1.2 Cost mitigation: a potential solution... 71
6.1.3 Funding... 72
6.2 Security of information and dissemination.. 72
7 Conclusion and recommendations 74
8 References.. 76
ANNEX A: Relevant definitions.. 79
ANNEX B: Available standards.. 86

Table of tables

Table 2-1: Physical properties of common nerve agents.. 12
Table 2-2: Physical properties of common blister agents... 12
Table 2-3: TICs and TIMs listed by hazard index 13
Table 2-4: Bacterial agents... 16
Table 2-5: Rickettsiae 17
Table 2-6: Viral agents... 17
Table 2-7: Biological toxins.. 18
Table 2-8: Physical properties of likely radiological agents 23
Table 2-9: Availability of likely radiological agents 24
Table 2-10: Masking of SNM with other radionuclides... 25
Table 2-11: Common explosives 32
Table 3-2: Factors That Affect Operator and System Performance....................................... 51
Table 3-3: Comparison of NFPA 1994 Class 1, Class 2, and Class 3..................................... 57
Table 4-1: Sample rating scheme 1 60
Table 4-2: Sample rating scheme 1 example 61
Table 4-3: Sample rating scheme 2 61
Table 4-4: Sample rating scheme 2 example 61
Table 4-5: Sample rating scheme 3 62
Table 4-6: Sample rating scheme 3 example 62
Table 4-7: Sample rating scheme 4 63

Table 4-8: Sample rating scheme 4 example ... 63
Table 5-1: Chemical characteristics table ... 66
Table 5-2: Biological characteristics table ... 67
Table 5-3: Radiological/Nuclear characteristics table ... 68
Table 5-4: Explosives characteristics table ... 69
Table B-1: List of available standards regarding explosives detection equipment ... 86
Table B-2: List of IEC standards regarding RN detection equipment ... 86
Table B-3: List of available ANSI standards regarding RN detection equipment ... 86
Table B-4: List of documents containing relevant IAEA standards ... 87

Table of Figures

Figure 2-1: A timescale for detection to specificity of a biological detector. ... 15
Figure 2-2: Explosives vapour pressures. ... 27
Figure 2-3: Trace detection technologies. ... 28
Figure 2-4: Bulk detection technologies. ... 30
Figure 3-1: Testing and Evaluation during product life cycle. ... 35
Figure 3-2: Explosive scenario E1 experimental setup. ... 43
Figure 3-3: The SITE Structure ... 47
Figure 3-4: High-level Total Architecture for Aviation Security. ... 49
Figure 3-5: Total Architecture for Aviation Security. ... 49
Figure 3-6: Role of the human operator in explosives detection. ... 50

1 Executive Summary

Today, the testing of CBRNE detection equipment is confined mostly to laboratory testing. This type of testing is conducted in highly controlled or ideal conditions. Therefore, the results of such testing should be considered as the upper bounds or best-case performance of a given CBRNE detector. For example, the probably of detection P_d of a handheld chemical detector yielded from a laboratory test should be used as the best possible result and not a "use-case" result. According to end-users, what is needed is an additional testing protocol that can yield this use-case result.

The purpose of this document is to create an operational testing framework. The operational testing framework (OTF) lays the groundwork for further development of an operational testing protocol for CBRNE detection equipment. As a framework, a major goal of OTF is to Illuminate many of the issues surrounding operational testing and to draw attention and initiate a focused discussion within the CBRNE stakeholder community on the usefulness of the suggested approach. In the following paragraphs, we describe at a high level the content of the OTF that supports our concept of operational testing.

Within the introduction, section 2, we present some background information. First, there is a discussion addressing the rationale behind the inclusion of operational test. Following that, thee objectives of each of the stakeholder groups involved (testing organizations, end-users, procurement organizations and manufacturers) are briefly discussed. We finish the section with a rather detailed description of each of the four focuses of the CBRNE detection field by explaining the general state of each field, threat materials involved, the most common technologies used for each specific field, and interference and simulant testing.

Section 3, represents the core of operational testing. It contains four sections: the concept, the scenarios, human factors, and the test and evaluation. The concept is where the focus is defined specifically the "performance difference". Essentially operational testing focuses on determining the difference between the laboratory performance of the detector and the operational performance. Next, the cornerstone of operational testing, the scenarios, are described. The scenarios will provide a script for the testing that will place the operator (end-user) and the detector under test in situations that mimic, as close as possible, the actual situations that can be encountered when using the detector in real operations. Human Factors Testing and Evaluation (HFTE) is described in subsection 3.3. The section provides a historical background, the SITE mnemonic, and an example of how HFTE is used. HFTE investigates the human-system interface and addresses issues such as usability, operational interaction, and situational stress. The final subsection is where some testing considerations are listed. The list of considerations is not complete but can serve as a sound starting point.

The next issues to be addressed are how to quantify/qualify the results of operational testing and how to report these results to the end-user. These are addressed in sections 4 and 5 respectively. The performance metrics and the report should be written is such as way as to provide the end-user with enough information to make an informed decision

regarding the capabilities and applicability of a given detector and be able of making a valid comparison of the available CBRNE detection devices without going into technical details that may be beyond their competence.
Cost is always a consideration when conducting testing of any kind. The inclusion of operational testing is no different. The cost/benefit of operational testing is presented in subsection 6.1. This subsection is not a scientific study of the issue but rather gives the reader some idea of the benefit gained through operational testing and also discusses briefly some ways to possibly mitigate the costs associated.

Subsection 6.2 deals with the dissemination of the OTF as well as the results of the testing. At present, the OTF as well as the results should be classified as PUBLIC. The rationale behind this is that the document should be disseminated to as large a number of the CBRNE stakeholder community as possible to ensure a useful debate regarding operational testing.

The OTF is closed with section 7 Conclusions and recommendations. A few take-aways from the OTF are: the threat from CBRNE incidents is a European Union security issue not a national security issue and should be treated appropriately; laboratory testing of CBRNE detection systems is not sufficient to give a complete picture of the capabilities of a detection system; the OTF is a starting point for an operational testing protocol not the destination; and several follow-on projects could be foreseen to develop the scenarios into scripts, test procedures further, as well as to address standardization of the operational testing protocol.

Acronyms specific to this document

ANSI American national standards Institute
BA Biological agent
CBRNE Chemical Biological Radiological Nuclear Explosive
CCD charge coupled device
CP Chemical protective
CW chemical warfare
EDS explosive detection system
FLAPS Fluorescence Aerodynamic Particle Sizer
GB sarin
HEU highly enriched uranium
HPLC High-Performance Liquid Chromatography
IDLH Immediately Dangerous to Life and Health
IED Improvised Explosive Device
IMS Ion Mobility Spectrometry
ISO International organization for standardization
LIBS laser-induced breakdown spectroscopy
NFPA National Fire Protection association
NQR nuclear quadrupole resonance
OPCW Organization for the prohibition of chemical weapons
PFNA pulsed fast neutron activation
PPE personal protective equipment
R&D research and development
RPM radiation portal monitors
SCBA self-contained breathing apparatus
SME subject matter expert
SPRM spectroscopic radiation portal monitors
TIC toxic industrial chemical
TNA thermal neutron activation
UAV Unmanned Aerial Vehicle
VBIED Vehicle Borne Improvised Explosive Device
WMD Weapons of Mass Destruction
ASAS Aerosol Size and Shape Analyzer
BWA biological warfare agent
CBW Chemical Biological warfare
CL Chemiluminescence
CT computed tomography
CWA chemical warfare agent
EU European Union
FTIR Fourier Transform Infrared
GC gas chromatography
HFTE human factors testing and evaluation
IC Ion Chromatography
IEC International Electrotechnical Commission
IEEE Institute of Electrical/Electronics Engineers
IR infrared
LD50 Lethal Dose for 50 % of Population
Mass Spectrometry
NPP nuclear power plant
NSD Neutron search detector
OT&E operational test and evaluation
PID Photoionization Detection
PRS portable radiation scanners
RID Radioisotope Identifiers
SAW surface acoustic wave
SITE situation, individual, task, and effect
SPRD spectrometric personal radiation detectors
TAAS total architecture for aviation security
TIM toxic industrial material
TR thermo-redux
UGV unmanned ground vehicle
WGPu weapons grade plutonium

2 Introduction

Today, the testing of CBRNE detection equipment is confined mostly to laboratory testing. This testing is conducted in highly controlled or ideal conditions. Therefore, the results of such testing should be considered the upper bounds of a given device characteristic. For example, the probably of detection P_d of a handheld chemical detector yielded from a laboratory test should be used as the best possible result and not a “use-case” result.

According to end-users, what is needed is an additional testing protocol that can yield this use case result. Operational testing is the only way to provide this data. In this type of testing the device under test is placed in situations that closely mimic the real world conditions that would be present when the device was actually used in a CBRNE incident. Variables such as temperature, humidity, altitude, and interferents should all be measured and controlled to ensure valid and reproducible results.

Additionally, there are important factors that are difficult to evaluate in bench tests. For example: do end-users find the detector user-friendly. Issues such as size, weight, operational placement, controls, and if it can be used without being an obstacle in the daily work are seldom considered. These so-called human factors testing should be introduced into the testing of CBRNE detection equipment. Issues such as man-machine interface, usability, and device placement should all be investigated. These human factors can be addressed within the operational testing protocol.

The bench testing is done by technically skilled personnel in a very controlled manner and environment to simplify technical considerations. The end-user is often required to handle various tasks, where using detectors is primarily for personal protection and not a main duty. The detectors may be used in different and varying environments.

Finally, operational testing should include end-user specific parameters (human factors like skill level etc.); a realistic environment and conditions for the test defined in a close to real scenario, and the results from operational testing should provide information on capabilities obtained with the equipment at the test.

Bench testing is done to obtain the detectors best performance in an ideal environment. Operational testing is performed to understand the capability obtained by the end-user.

2.1 Objectives to perform operational testing

General objectives

The specifications obtained during bench tests are not inherently valid in an operational environment. Sometimes the specifications are valid but the performance in the field can differ significantly. This difference would be of an academic nature if all CBRNE equipment behaves similarly, but that is not the case. In fact, the differences can be large. The detector performance is dependent upon aspects like selected detection technique, sampling method, engineering skill, analysis method and on which substances are to be detected. Often manufacturers demonstrate detector performance with compounds for which the detector has good sensitivity and selectivity rather than a broad range of compounds. If this is not known by the customer, generalizations extended to other compounds and comparisons made to other instruments can be incorrect. The result may be that the customers' expectations of the product will be unwarrantedly high and they may become disappointed when the equipment is put into operation. A bad acceptance by the end-user may result in that the equipment won't be used as intended and that the expected capability will be omitted. The procurement may also be considered unfair by the competing manufacturers who may do broader testing. In both cases there will be a waste of time and money.

In the United States armed forces both bench tests and operational test are used in Joint Procurement projects. The bench tests are used in the beginning of the procurement process to evaluate the state of the art of the technology and to select manufacturers that can show promising results to the final test referred as the Joint Field Trial. Prior to the field trial, the participating manufacturers get information on how the test will be performed and what will be evaluated. During the field trial, they will not receive any additional information or guidance on what is taking place. After each day they hand in the results obtained from their equipment which will be scrutinised by the testing authority. The system or systems with the best scores in the field trial will be selected to go onto the next step in the procurement process. A pre-series is often developed and evaluated by military units. These units may give the green light to series production or present corrections or new features that need to be made prior to series production.

Objectives for procurement organizations

The procurement process is often a result of a growing demand for a new or improved capability. This capability may be achieved in several ways; by procurement of a new detector, by improving the operational proceedings with the present equipment, by education and training of end-users and/or on a management level. In some cases a new detector is not enough to obtain the wanted capability. However, this is difficult to realise from reading the specifications from manufacturers. The procurement is done by a purchasing department or sometimes by a different governmental agency, sometimes having limited knowledge in the usage of the equipment and in technological matters. Operational testing could be done prior to procurement to evaluate why the capability desired can't be obtained with the existing equipment. It could also be very valuable if new equipment has been tested in an operational environment to demonstrate that the claimed detector performance is not only obtained at bench tests, but in real usage of the equipment as well.

Objectives for end-users

The end-users have different demands on CBRNE equipment depending on their tasks. Some end-users need equipment for personal protection and some to ensure public safety. The operational environment can vary from fixed sites indoors to mobile outdoor environments. Fortunately, first responders do not experience CBRNE threats very often. But that makes it even more important to put very high demands on CBRNE equipment by making them easy to use and preventing them from being an obstacle in the daily work. If and when a CBRNE event occurs it will have serious consequences that force the end-user to make difficult decisions and to do potentially life threatening tasks. Thus, it is important that the end-user have confidence that they will obtain the required capabilities with their CBRNE equipment to do the work.

Objectives for manufacturers
A manufacturer's first objective is to make money on their product. However, customer relations and feedback are also critical elements to a successful business. Often manufacturers have difficulty in obtaining the end-users opinions on product performance under operational conditions. There are examples of manufacturers forming user groups where questions are raised and the feedback used by the company to improve product capabilities and services. Because procurement is based on product specification, not on obtainable end-user capability, this feedback is important. The manufacturer is required to have satisfied customers, but since the end-user is not involved in the procurement process it may be more important to obtain good scores in product bench tests and to provide a product with a cheap initial price, than to provide equipment that really works and have a low maintenance cost. In the long run, it will be important to learn more about end-user needs and operational testing can be one way to obtain it.

2.2 Principles of CBRNE detection

In this report we define CBRNE detection as the ability to immediately indicate a threat, typically within seconds, whereas CBRNE identification is defined as identification of a chemical, biological, radiological/nuclear or explosive substance to a specified level. B detection is done on aerosol particles in the size range of one to ten micrometers. C, RN and E detection on the other hand may be done for substances in gas, aerosol, liquid and solid phases. In E detection, bulk and trace detection can be distinguished. For bulk detection, an objects unspecific properties like the shape and size or materials composition (metals, electronic plates, wires inside a parcel) are inspected by x-ray or other image producing technologies, while trace detection is very much similar to chemical detection analysing substance-specific properties to find hazardous (explosive) materials in very small quantities. RN detection makes use of the physical property of ionizing radiation (i.e. produce ions via radiation). As such these detectors are not dependent on contact with the medium, but can detect radiation from short (alpha radiation) or far distance (gamma radiation).

Detectors sampling and analysing the air in close proximity of its own location are named point detectors and can be handheld, mobile or integrated in fixed installations. Remote detectors are also point detectors, but they are remotely controlled and supervised from a distance. Standoff detectors are detecting substances in the air at a distance. In some cases a light source (often a laser) is used to make the standoff detection possible, and sometimes just to enhance its performance. There are at present commercial standoff detectors for chemicals but for biological aerosol there only exist prototypes and demonstrators in different technological maturity.

First responders often have several areas of responsibility; for example customs should be able to find drugs, explosives, radioactive material and CWA. If specialized detectors are used for each task, maintenance and training become a burden. This is understood by manufacturers of detection instruments, providing handheld detectors with several sensors. Examples of sensors that use to complement each other are ion mobility spectrometer (IMS), a photo-ionization detector (PID), electrochemical cells, surface acoustic waves (SAW) sensors and semiconductor gas sensors. At a fixed location, a building sensor network of more specialized detectors is a better solution. In both cases, integrated sensors in a device or integrated detectors in a network, the sensors are selected to complement each other.

2.3 Specifics of chemical detection

The development of C detectors has been going on for several decades. In many countries, the developments have evolved from the threat scenarios of the Cold War. Back then there were a few very toxic substances, most of them were put on the OPCW[1] list of chemical warfare agents, which were supposed to be used in huge quantities and over large areas. The detection of this type of hazards has been successfully solved by detection papers, enzymatic detection tickets, flame photometric detection and ion mobility spectrometry. Today the threats are not primarily originating from known national chemical warfare programs, but include also terrorists and accidents opening up for a huge number of less toxic compounds. Thus, it has become more difficult to find adequate detection techniques because the number of agents has grown significantly and a large dynamic range is required to detect both trace amounts of chemical warfare agents (CWA) and toxic industrial chemicals (TIC).

Stand-off detection on long distances is done with Fourier Transform Infra Red (FTIR), but on shorter distances Raman spectroscopy and laser-induced breakdown spectroscopy (LIBS) may be used. Passive FTIR standoff detectors use the natural blackbody radiation from the temperature difference between the background and the gas cloud to detect chemical signatures in the infrared spectral region. The sensitivity is proportional to the temperature difference between the gas and the temperature of the background and is about two Kelvin degrees on average. Active systems have an IR light source (laser or lamp) providing an increase in temperature contrast of about three orders of magnitude. The advantage of passive systems is that they are smaller, lighter, cheaper, and consume less power than the active systems. The passive systems can survey an area by scanning in the FTIR spectra pixel by pixel or by hyper-spectral detection where a detector array (CCD) is used to obtain simultaneous IR spectra in each pixel of the picture. Active systems are scanning or fixed.

There are a few strategies in use to deal with the difficulties of the much larger threat list. In one end of the range, there are generic sensors with very low specificity alarming if there is a change in chemical gas concentration. In the other end of the range there are basically field adapted laboratory instruments, using technologies (mass spectroscopy (GC-MS), Fourier Transform Infra Red (FTIR) spectroscopy and Raman spectroscopy) with very high specificity.

[1] Organisation for the Prohibition of Chemical Weapons: see http://www.opcw.org

2.3.1 Typical agents

Table 2-1 and 2-2 show the physical properties of some common CWA compared to water. These properties are important for how the chemicals can be detected in terms of physical state (solid, liquid, gas or aerosol), water solubility and equilibrium gas concentration (in terms of volatility). What can be noted is that sarin (GB) is as volatile as water, but VX is about 2,000 times less volatile. This makes it much harder to detect VX than GB and that there will be less needs for decontamination of GB than for VX. Unfortunately, the risk hazard for VX is about ten times higher than GB. Operational requirements for chemical detectors should be based on how the detector is to be used and on an acceptable level health hazards. The US Army has written a comprehensive guidance for requirements of detection limits and alarm limits, based on health hazards (USA CHPPM Technical Report No. 64-FF-07Z2-07). This report can be used for acquisition of both civilian and military C/TIM detectors, but depending on different acceptable risks of health hazards the requirements may be different for detectors used in civilian and military contexts.

Table 2-1: Physical properties of common nerve agents

Property	GB	GA	GD	GF	VX	Water
CWA name	Sarin	Tabun	Soman	Cyclosarin	VX	
Molecular weight	140.1	162.3	182.2	180.2	267.4	18
Density, g/cm^3*	1.089	1.073	1.022	1.120	1.008	1
Boiling point, °C	158	240	198	239	298	100
Melting point, °C	-56	-8	-42	-30	< -51	0
Vapour pressure, mm Hg *	2.9	0.07	0.4	0.06	0.0007	23.756
Volatility, mg/m^3 *	22 000	610	3 900	600	10.5	23 010
Solubility in water, % *	Miscible with water	10	2	~2	Slightly	NA

(Source: Fatah et al. 2007a)

Table 2-2: Physical properties of common blister agents

Property	HD	HN-1	HN-2	HN-3	L	Water
Molecular weight	159.1	170.1	156.1	204.5	207.4	18
Density, g/cm^3	1.27 at 20 °C	1.09 at 25 °C	1.15 at 20 °C	1.24 at 25 °C	1.89 at 20 °C	1 at 25 °C
Boiling point, °C	216	194	75 at 15 mm Hg	256	190	100
Freezing point, °C	14.4	-52	-65	-3	18 to 0.2	0
Vapour pressure, mm Hg	0.072 at 20 °C	0.24 at 25 °C	0.29 at 20 °C	0.011 at 25 °C	0.394 at 20 °C	23.756 at 25 °C
Volatility, mg/m^3	610 at 20 °C	1520 at 20 °C	3580 at 25 °C	121 at 25 °C	4480 at 20 °C	23,010 at 25 °C
Solubility in water, %	<1 %	Sparingly	Sparingly	Insoluble	Insoluble	1 at 25 °C

(Source: Fatah et al. 2007a)

Chemical detectors are being used for personal protection, for monitoring an area or a site, to obtain risk areas after an attack or accident, to find a source and shut it down and in the analysis chain to find hot spots to take samples from. The detector requirements needed to obtain those capabilities is often very different. In practice, many organizations use the same detectors to solve all problems. This is understandable in terms of limited budgets, limited time for training and maintenance; but it is a compromise that can give a false security or cause mistrust among the end-users.

2.3.2 TIC's and TIM's

There are toxic chemicals being used in large quantities by the industry. Some of them are stored and transported as condensed gas under high pressures. A leak from this kind of gas tanks or cylinders may cause mass casualties. Those chemicals are in the list of compounds with high hazard index in Table 2-3. The growing risk of terrorist attacks where available toxic materials can be used have caused the list of possible risk chemicals to grow. However, the risk for mass casualties is still limited to a few chemicals depending on physical properties.

Table 2-3: TICs and TIMs listed by hazard index

High	Medium	Low
Ammonia**	Acetone cyanohydrin	Allyl isothiocyanate
Arsine*	Acrolein	Arsenic trichloride
Boron trichloride	Acrylonitrile	Bromine**
Boron trifluoride	Allyl alcohol	Bromine chloride
Carbon disulfide	Allylamine	Bromine pentafluoride
Chlorine**	Allyl chlorocarbonate	Bromine trifluoride
Diborane	Boron tribromide	Carbonyl fluoride
Ethylene oxide	Carbon monoxide*	Chlorine pentafluoride
Fluorine	Carbonyl sulfide	Chlorine trifluoride
Formaldehyde	Chloroacetone	Chloroacetaldehyde
Hydrogen bromide	Chloroacetonitrile	Chloroacetyl chloride
Hydrogen chloride**	Chlorosulfonic acid	Crotonaldehyde
Hydrogen cyanide*	Diketene	Cyanogen chloride*
Hydrogen fluoride	1,2-Dimethylhydrazine	Dimethyl sulfate
Hydrogen sulfide	Ethylene dibromide	Diphenylmethane-4,4'-diisocyanate
Nitric acid, fuming	Hydrogen selenide	Ethyl chloroformate
Phosgene**	Methanesulfonyl chloride	Ethyl chlorothioformate
Phosphorus trichloride	Methyl bromide**	Ethyl phosphonothioic dichloride
Sulfur dioxide	Methyl chloroformate	Ethyl phosphonic dichloride
Sulfuric acid	Methyl chlorosilane	Ethyleneimine
Tungsten hexafluoride	Methyl hydrazine	Hexachlorocyclopentadiene
	Methyl isocyanate**	Hydrogen iodide
	Methyl mercaptan	Iron pentacarbonyl
	Nitrogen dioxide	Isobutyl chloroformate
	Phosphine**	Isopropyl chloroformate
	Phosphorus oxychloride	Isopropyl isocyanate
	Phosphorus pentafluoride	n-Butyl chloroformate
	Selenium hexafluoride	n-Butyl isocyanate
	Silicon tetrafluoride	Nitric oxide
	Stibine	n-Propyl chloroformate
	Sulfur trioxide	Parathion
	Sulfuryl chloride	Perchloromethyl mercaptan

High	Medium	Low
	Sulfuryl fluoride**	sec-Butyl chloroformate
	Tellurium hexafluoride	tert-Butyl isocyanate
	n-Octyl mercaptan	Tetraethyl lead
	Titanium tetrachloride	Tetraethyl pyrophosphate
	Trichloroacetyl chloride	Tetramethyl lead
	Trifluoroacetyl chloride	Toluene 2,4-diisocyanate
		Toluene 2,6-diisocyanate

* Blood agent ** Choking agent (Source: Fatah et al. 2007a)

2.3.3 Simulants, test agents and interferents

Simulants are being used for test and evaluation of detectors when the use of CWA should be too expensive, toxic or noxious. In outdoor tests simulants are commonly used. The simulants have similar chemical and physical properties to CWA, but are less toxic. When choosing a stimulant the goal is to find a substance that is as similar as possible to the substance which is classified as a CWA by the detector. Depending on the detection technique being used at the test, the CWA stimulants may vary. The flame photometric detector AP2C classifies compounds containing phosphorus as nerve agents and sulphur as mustard gas or VX. Thus, simulants for AP2C should contain phosphorus and/or sulphur having similar physical properties as the CWA they mimic. FTIR instruments detect molecular vibrations, which require that the stimulant has similar molecular structure as the CWA. The development of detectors with several kinds of integrated sensors makes it difficult to find adequate simulants, which may point in a direction to do more test and evaluation with CWA. Simulants are less toxic than CWA, but often still too toxic to be used in large quantities for training or large scale tests due to environmental regulations. Test agents can be detected by the instrument and have similar physical properties to CWA, but the chemical structure maybe very different.

There are similarities between simulants and interferents, since both are detected as CWA. The difference is that interferents are compounds present in the operational environment causing false positive detector alarms. The origin of interferents is lacking specificity to the threat agents. The number of possible interferents grows for every new substance added to the detection library. Combinations of different detection techniques may theoretically reduce the number of interferents. False alarms are not accepted by end-users. The desired demand from end-users is that manufacturers should prove that the detector won’t cause false positive alarms due to interferents. This is a claim that is impossible to achieve, since there are so many substances in use that possible could cause false alarms, by themselves or in mixtures of other substances. In this report operational testing is suggested to at least get an idea of how big problem interferents are in a specific situation.

2.4 Specifics of biological detection

B detection is primarily done for protective reasons. Even though most of today’s B detectors still give many false alarms, it is recommended that a warning from a B detector should start sample collection to enable confirmation by a fast identification method, as for example a biosensor based on an immunological method, before giving an alarm. Detection of contagious levels of biological warfare agents (BWA) is genuinely difficult. Already very low doses of BWA in air can infect humans, so the detection system must be very sensitive. The system also needs to be fast so that precautionary measures can be taken before people have been exposed to the threat. To complicate the task even further, there are many harmless naturally occurring biological particles that are hard to distinguish from the hazardous ones. This is one of the strongest reasons of doing the detection on individual aerosol particles, not at an average over time or volume when the signal from the detector is a result of several particles. Averaging lowers the limit of detection, but may at the same time disguise a positive signal. Consequently, it is not a trivial task to construct protection systems against the threat of BWA. No single sensor or technology fulfils all the requirements for sensitivity; speed and specificity (distinguish between harmless and hazardous particles). A detection instrument gives alarm within seconds if the physical properties of an aerosol resemble particles of biological origin. The alarm often automatically starts an aerosol sampler. Immunological methods recognize surface properties of the agents and genetic methods target specific nucleic acid sequences of the agents. The genus level give information on which kind of agent that is present or absent in the sample. However, the species or sub species level is needed to distinguish between virulent and harmless forms of the agent.

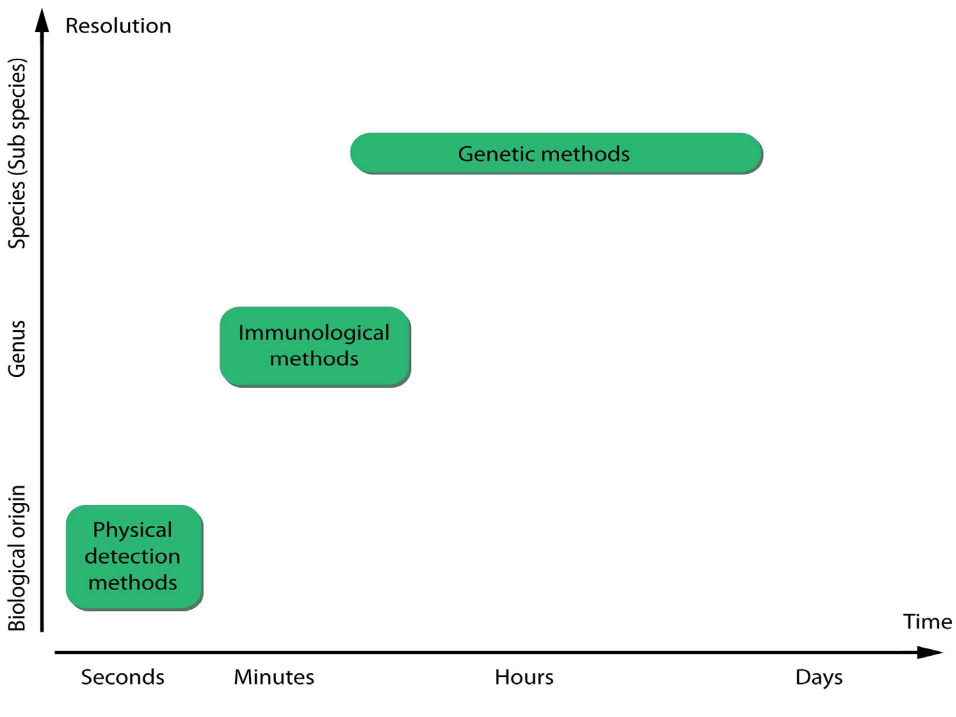

Figure 2-1: A timescale for detection to specificity of a biological detector.

Many BWA detection systems therefore combine different sensors to achieve the best performance possible (Fitch et al., 2003). These systems normally have an initial warning or trigger detector that continuously monitors the air to achieve a fast response time. The trigger detectors measure some inherent property of the dry aerosol particles and warn personnel and trigger further analysis with other sensors. Examples of warning detectors are the Aerosol Size and Shape Analyzer (ASAS) that measures the particle shape from laser scattering (Clark et al., 1993, Kaye et al., 1991, Kaye et al., 2000), the Fluorescence Aerodynamic Particle Sizer (FLAPS) system that measure size and presence of ultraviolet (UV) induced fluorescence (Hairston et al., 1997, Ho, 1996, Ho and Spence, 1998) and the Biological Alarm Monitor (MAB) which measure the elemental decomposition by flame spectrophotometry (Lancelin et al., 1999, Lancelin et al., 2004). These detectors can reach close to real-time warning but have relatively low specificity, sometimes resulting in false alarms.

2.4.1 Typical agents

There are many lists with typical agents that need to be detected by a biodetector. In general the typical agents are bacterial agents, viral agents and toxins. An extensive list of typical agents is given in Table 2-4 through
Table 2-7.

Table 2-4: Bacterial agents

Bacterial Agent	Disease	Method of Dissemination	Treatment	Potential as a Bio Weapon
Bacillus anthracis	Anthrax	1. Spores in aerosol 2. Sabotage (food) 3. Cutaneous—contact with animal product	Antibiotics approved for anthrax are ciprofloxacin, tetracyclines (including doxycycline), and penicillin	High
Brucella abortus, B. melitensis, B. suis, B. canis	Brucellosis	1. Aerosol 2. Sabotage (food)	Antibiotics	Unknown
***Escherichia coli serotype* (O157:H7)**	Diarrhea, hemolytic uremic syndrome	1. Water 2. Food supply contamination	Antibiotics available; most recover without antibiotics within 5 d to 10 d; do not use anti-diarrheal agents	Unknown
Francisella tularensis	Tularemia	1. Aerosol 2. Water / food contamination 3. Ticks	Antibiotics: parenteral antimicrobial therapy recommended A vaccine for tularemia is under review but is not currently available	High, if delivered via aerosol form (highly infectious, 90 % to 100 %)
Vibrio cholerae	Cholera	1. Sabotage (food and water)	Replenish fluids and electrolytes; a pre-packaged oral rehydration solution is available	Not appropriate for aerosol delivery
Burkholderia Mallei	Glanders	1. Aerosol 2. Cutaneous	Drug therapy (streptomycin and sulfadiazine) is effective	Unknown
Pseudomonas pseudomallei	Melioidosis	1. Food contamination (rodent feces) 2. Inhalation	Antibiotics (doxycycline, chlorothenicol, tetracycline) and sulfadiazine	Moderate—no vaccine available

Bacterial Agent	Disease	Method of Dissemination	Treatment	Potential as a Bio Weapon
Yersinia pestis	Plague (pneumonic and bubonic)	1. Aerosol (pneumonic) 2. Infected fleas (bubonic and pneumonic)	Antibiotics: streptomycin (or gentamicin), tetracyclines and chloramphenicol	High– highly infectious, esp. pneumonic (aerosol) form
Salmonella typhi	Typhoid fever	1. Contact with infected person 2. Contact with contaminated substances	Antibiotics (amoxicillin or cotrimoxazole) shorten period of communicability and cure disease rapidly	Not likely to be deployed via aerosol; more likely for covert contamination of water or food

(Source: Fatah et al. 2007b)

Table 2-5: Rickettsiae

Biological Agent	Disease	Method of Dissemination	Treatment	Potential as a Bio Weapon
Rickettsia typhus	Endemic Typhus	Aerosol	Antibiotics (tetracycline and chloramphenicol); supportive treatment and prevention of secondary infections	Uncertain—broad range of incubation (6 d to 14 d) period could cause infection of force deploying BA
Rickettsia prowazekii	Epidemic Typhus	Aerosol	Antibiotics (tetracycline and chloramphenicol); supportive treatment and prevention of secondary infections	Uncertain—broad range of incubation (6 d to 14 d) period could cause infection of force deploying BA
Coxiella burnetii (Rickettsia burnetti)	Q Fever	1. Sabotage (food supply) 2. Aerosol	Tetracycline (500 mg/ 6 h, 5 d to 7 d) or doxycycline (100 mg/ 12 h, 5 d to 7 d) also, combined Erythromycin (500 mg/ 6 h) and rifampin (600 mg/d)	Highly infectious if delivered in aerosol form; dried agent is very stable; aerosol form is stable
Rickettsia rickettsii	Rocky Mountain Spotted Fever	Aerosol	Antibiotics—tetracycline or chloramphenicol	Unknown

(Source: Fatah et al. 2007b)

Table 2-6: Viral agents

Biological Agent	Disease	Method of Dissemination	Treatment	Potential as Bio Weapon
Filovirus	Marburg Hemorrhagic Fever	Aerosol	No specific treatment exists; severe cases require intensive supportive care	High—
Filovirus	Ebola Hemorrhagic Fever	Direct contact Aerosol (BA)	No specific therapy; supportive therapy essential	Unknown—

Biological Agent	Disease	Method of Dissemination	Treatment	Potential as Bio Weapon
Tacaribe Virus complex Arenavirus	Argentine Hemorrhagic Fever (Junin)	Not known	No specific therapy; supportive therapy essential	Unknown
Phlebovirus	Rift Valley Fever	Mosquito-borne; aerosols or droplets	No studies, but IV ribavirin (30 mg/ kg/6 h for 4 d, then 7.5 mg/kg/8 h for 6 d) should be affective	Difficulties with mosquitoes as vectors
Variola major, Orthopoxvirus	Smallpox	Aerosol	Vaccinia immune globulin (VIG) and supportive therapy	Possible, especially since routine smallpox vaccination programs have been stopped
Flaviviruses	Yellow Fever Virus	Mosquito-borne Aerosol	No specific treatment; supportive treatment	High, if efficient dissemination device is employed
Flaviviruses	Dengue Fever Virus (DEN-1, DEN-2, DEN-3, and DEN-4)	Mosquito-borne (*Aedes aegypti*)	No specific therapy; supportive therapy essential	Unknown
Nairovirus	Congo-Crimean Hemorrhagic Fever Virus	Insect vectors	No specific treatment	Unknown
Alphavirus	Venezuelan Equine Encephalitis	Aerosol	Supportive treatments only; there is a vaccine for laboratory workers	High—weaponized as both liquid and dry forms for aerosol distribution

(Source: Fatah et al. 2007b)

Table 2-7: Biological toxins

Biological Toxins			
Toxin	**Method of dissemination**	**Treatment**	**Potential as Bio Weapon**
Botulinum toxin	1. Aerosol 2. Sabotage (food and water)	Antitoxin with respiratory support (ventilation)	Not very toxic via aerosol route; extremely lethal if delivered orally
Staphylococcal enterotoxin B (SEB)	1. Sabotage (food supply) 2. Aerosol	Pain relievers and cough suppressants for mild cases; for severe cases, may need mechanical breathing and fluid replenishment	Moderate—could be used in food and limited amounts of water (for example, at salad bars); LD50 is sufficiently small to prevent detection
T-2 mycotoxins	1. Aerosol 2. Sabotage	No specific antidote or therapeutic regimen is available; supportive and symptomatic care	High—used in aerosol form (“yellow rain”) in Laos, Kampuchea and Afghanistan (through 1981)
Ricin	1. Aerosol 2. Sabotage (food & water)	Oxygen, plus drugs to reduce inflammation and support cardiac and circulatory functions	included on prohibited Schedule I chemicals list for Chemical Weapons Convention; high potential for use in aerosol form

Biological Toxins			
Toxin	**Method of dissemination**	**Treatment**	**Potential as Bio Weapon**
Saxitoxin	In biological scenario, inhalation or toxic projectile	Induce vomiting, provide respiratory care, including artificial respiration	Moderate, aerosol form is highly toxic

(Source: Fatah et al. 2007b)

From this list it should be obvious that testing and evaluation of a biodetector is a difficult task and that the agents to be tested against are defined by the sensor technology tested and the specific wishes of the client.

2.4.2 Simulants and interferents

Due to the high risk associated with aerosolizing living biological agents, simulants are normally used to test a biodetector. Typical simulants are:

Bacillus globigii (BG): BG are spores of the bacterium Bacillus globigii or with the current scientific name Bacillus atrophaeus. Usually, testing-centres acquire BG from authorized suppliers but more frequently laboratories are growing BG spores themselves. BG can be aerosolized as a dry powder or in a liquid form. BG spores are used as model for Anthrax.

Bacillus thuringiensis (BT): An alternative for BG spores are spores from Bacillus thuringiensis var. kurstaki aizawai. BT can be bought as a dry commercial biological insecticide (Turex 50 WP).

Erwinia herbicola (EH): EH are vegetative cells of Erwinia herbicola or with the current scientific name Pantoea agglomerans. EH is grown in the laboratory and aerosolized as a liquid. EH is renowned for its instability in air at low relative humidity. EH is used as a model for Gram-negative bacteria like Yersinia pestis.

MS2: MS2 is a bacteriophage (a virus for bacteria). It is very small and is propagated in the laboratory in the bacterium Escherichia coli. Although the disadvantage of the small size of MS2 compared to real threat viruses, it is frequently used in testing biodetectors since it’s concentration can be easily determined.

Baculovirus: with the scientific name Cydia pomonella granulovirus (CpGV), has been used as a simulant for Smallpox virus, instead of MS2 bacteriophage. Both Baculovirus and Smallpox virus have a double stranded DNA genome, whereas MS2 has a single-stranded RNA genome. Considering viral particle size and morphology, Baculovirus would also be more closely resembling to Smallpox virus. Baculoviruses are more difficult to culture than MS2, except if you are used to culture insect cells or insect larvae. Therefore, DNA methods are usually applied to determine the concentration of this virus.

Ovalbumin (OV) is a protein form chicken eggs and can be commercially obtained in different grades. OV serves as a model for toxins. Although simulants are commonly used, killed real treat agents are sometimes used in field trials. Interfering substances that are used by testing-centres are diesel exhaust fumes, dust (e.g. standardized (Arizona road dust), and smoke.

2.5 Specifics of radiological/nuclear detection

Large varieties of instruments for R/N applications (i.e. instruments for the detection of ionizing radiation and nuclear materials) are available on the market and dedicated institutions are employing even more for specific purposes. Some of them have proven their capabilities under normal conditions and in the aftermath of past unplanned events, some have evolved based on the lessons learned from these events. Especially the technology for detecting radioactive materials has developed rapidly in recent years.

There is a user-driven trend in hazard assessment to combine dose rate measurement, localization, and radionuclide identification into a single handheld instrument using multiple radiation detectors. Compared to pocket-type instruments, of which only those that employ scintillation detectors are sensitive enough for the application as a locating device, handheld instruments provide greater sensitivity of detection. The downside is that they are usually heavier and more expensive and thus they are most often used for detection in targeted search situations of specified consignments. For example, they would be chosen when there is a suspicion that a radioactive source already exists, to localize the source, to measure the dose rate; or to identify the radionuclide.

With the requirement for increased sensitivity and enhanced energy resolution of handheld radionuclide identifiers, new room temperature detector materials have to be investigated and appropriate and dependable software to analyze and interpret the sometimes complex spectra generated by these detector systems has to be developed. Another challenge is posed by the degradation of spectral lines through shielding, which may lead to misidentifications.

A very comprehensive overview about different kinds of radiation detectors is available from (Engelbrecht et al. 2006) which was compiled for the IMPACT project. It includes information on personal direct reading dosimeters, radiation pagers; handheld survey meters for alpha, beta, and gamma detection and neutron counters; handheld radionuclide identifiers; mobile laboratories and portable identification instruments as well as stationary monitoring equipment.

Available radiation detection equipment relevant for nuclear security and specifically for border monitoring purposes is categorized according to the typical use of the instruments. The short overview below is taken from the I-Ispra - Illicit Trafficking Radiation Assessment Program (ITRAP+10 Project) description (JRC 2010).

- Radioisotope Identifiers (RID) are multipurpose handheld instruments used that can detect, locate, and identify radioactive/nuclear materials as well as to provide reasonably accurate measurements of the gamma dose rate and the measured neutron count rate (if applicable).

- Highly Sensitive Neutron Search Detectors (NSD) are handheld instruments designed for high neutron detection sensitivity. They combine limited size and weight to allow for handheld operation for a sufficiently long time. Their purpose is to detect and locate neutron emitting radioactive material. They were introduced to complement Radiation Portal Monitors with their greater neutron sensitivity enabling operators to better verify neutron alarms. NSD can be used as primary search and detection devices to search pedestrians, packages, cargo and vehicles or as improvised automated neutron monitors by using the built in alarm capability.
- Portable Radiation Scanners (PRS) have the highest sensitivity of all available portable systems and are often used in a backpack design. The applications of PRS are mobile radiation screening for pedestrians, vehicles, and cargo in public urban areas. Additionally, they can be employed at border crossing points where the deployment of standard fixed-installed RPM is not feasible or practical. The PRS can also be used as a primary tool for detection of hidden sources or radiological area reconnaissance (i.e. the inspection of an area to find out details about the possible threat situation). Being similar in its intended application to an RID, the instrument has the same main functions: detection, location, dose rate indication, and radionuclide identification. The instrument design however differs significantly from that of RID, originating from its larger size and intended use for cover detection.
- Spectrometric Personal Radiation Detectors (SPRD) are pocket-sized devices that are worn on the body for the purpose of rapid detection and identification of radioactive materials.

Fixed instruments are typically used at borders control points, airports, ports, and at the entrance of critical infrastructures.

- Radiation Portal Monitors (RPM) are fixed installed radiation detection systems designed for the screening of vehicles and containers for gamma and neutron radiation. They are designed to give an alarm in the presence of increased radiation. They are not intended to provide identification of radionuclides present.
- Spectroscopic Radiation Portal Monitors (SRPM) are fixed installed systems, which can detect and also identify a radionuclide causing an alarm. They can indicate the level of threat by providing a green, yellow, or red light alarm which derived from the measured radionuclide activity. SRPM are also able to determine the type of nuclide present whether it is: medical; naturally occurring radionuclides; specific nuclear material; industrial sources.

2.5.1 Typical technologies used by these types of detectors

For the different designs listed above a number of detection technologies are available, each having specific advantages and limitations. A short summary of detector types is given in Annex B of the ANSI N42.48-2008 Standard (ANSI 2008) together with reference to the relevant testing standards.

- *Sodium Iodide (NaI) scintillation detectors:* These detectors are available in large sizes such that they have both high efficiency and moderate energy resolution. They are operated at room temperature. These detectors are used for their high efficiency of light output per photon incident. Test procedures for systems using scintillation detectors can be found in ANSI N42.12-1994. Cesium Iodide (CsI) Scintillation detectors have very similar properties and usage.
- *Cadmium-Zinc-Telluride (CZT) semiconductor detectors:* CZT and other wide band-gap semiconductor detectors are semiconductor detectors that can be operated at room temperatures. At this time they are small physically and therefore have low efficiency. They have good energy resolution though somewhat poorer than that of Germanium detectors. Standard test procedures for these detectors are given in ANSI N42.31-2003[2].
- *Germanium gamma-ray detectors:* These detectors have very high energy resolution and are currently of sufficient size to have also high efficiency. They must be operated at cryogenic temperatures (i.e. cooled with liquid nitrogen to extremely low temperatures). Test procedures for these detectors are given in IEEE STD 325-1996[3].
- *Semiconductor charged-particle detectors:* These detectors are capable of high resolution measurements of charged particles. Test procedures for these detectors are given in IEEE STD 300-1988[4].
- *Geiger-Mueller counters:* These are widely used for radiation detection and intensity measurements (usually beta particles and gamma rays, but certain models can detect alpha particles). An inert gas-filled tube (usually helium, neon or argon with halogens added) briefly conducts electricity when a particle or photon of radiation makes the gas conductive. The tube amplifies this conduction by a cascade effect and outputs a current pulse, which is then often displayed by a needle or lamp and/or audible clicks. Modern instruments can report radioactivity over several orders of magnitude[5]. Test procedures for these detectors are given in IEEE STD 309-1999/ANSI N42.3-1999[6].
- *Ionization chambers:* These are highly accurate detectors for gross measurement of radiation. They are operated at room temperature. Test procedures for these detectors are given in ANSI N42.13-1986[7].
- *Plastic scintillator detectors:* These detectors are particularly useful for portal monitors. Standards and standard measurement procedures have not yet been developed.
- High-pressure ^{3}He proportional counters: These are particularly useful for neutron detection and are commonly used in portal monitors.

---

[2] ANSI N42.31-2003 American National Standard for Measurement Procedures for Resolution and Efficiency of Wide-Bandgap Semiconductor Detectors of Ionizing Radiation

[3] IEEE Std 325™-1996 (Reaff 2002), IEEE Standard Test Procedures for Germanium Gamma-Ray Detectors

[4] IEEE Std 300™-1988, IEEE Standard Test Procedures for Semiconductor Charged-Particle Detectors.

[5] Definition taken from Internet: http://en.wikipedia.org/wiki/Geiger_counter

[6] IEEE Std 309™-1999/ANSI N42.3-1999, IEEE Standard Test Procedures and Bases for Geiger-Mueller Counters.

[7] ANSI N42.13-1986 (R1993), American National Standard for Calibration and Usage of "Dose Calibrator" Ionization Chambers for the Assay of Radionuclides

2.5.2 Maturity of the technology for field use (application for field use)

RN detection technologies have been developed over the last years to suit specific needs of different operational needs. Therefore, especially in comparison to detection systems for other threats (B, C, E), RN detectors have a very high technological readiness and quite a variety of different designs is available on the market to fit specific user needs.

2.5.3 Typical agents (to be used in a "dirty-bomb" scenario)

Radionuclides are characterized by the type of radiation they emit during physical decay (alpha, beta, gamma radiation, neutrons) and their physical half-life, i.e. how fast they decay. While alpha radiation can be shielded by a thin cover like a sheet of paper, gamma radiation can only be effectively shielded by solid materials like concrete or metal and it needs thick layers to substantially reduce external radiation of strong gamma sources (beta radiation is intermediate). For terrorist purposes only a few of all the radionuclides available are of practical use because they need to have a comparatively longer half-life (otherwise the spread contamination disappears very quickly without the necessity of counteractions). E.g. a half-life of 7 days (e.g. ^{131}Iodine) means that due to the physical properties of the material radioactivity is reduced to the half within a week. Typically after 7 half-lives (due to exponential decay) only 0.1% of the original radioactivity remains. This excludes many of the commonly used short-lived medical radionuclides. In contrast to low danger of external radiation, which is associated with alpha-emitters, they are very critical if incorporated (by inhalation, ingestion, absorption through skin lesions or mucous membranes) in terms of potentially adverse health effects (stochastic risk of cancer generation). In Table 2-8: Physical properties of likely radiological agents: a list of likely radiological agents to be used for terrorist activities (e.g. dirty bomb) has been compiled from different sources.

Table 2-8: Physical properties of likely radiological agents

Name		**main radiation emitted**	**Toxicity (Inhalation) (eff. dose coeff. [Sv Bq^{-1}]***	**Toxicity (external radiation) ***	**Volatility (at 20°C)**	**Water solubility**	**Physical half-life**
Americium	^{241}Am	alpha (gamma)	4.2 E-5	low	no	low	432 a
Uranium	^{238}U	alpha	2.9 E-6	low	no	low	4.47 E+9 a
Uranium	^{235}U	alpha	3.1 E-6	low	no	low	7.04 E+8 a
Plutonium	^{238}Pu	alpha	4.6 E-5	low	no	low	87.7 a
Plutonium	^{239}Pu	alpha	5.0 E-5	low	no	low	2.41 E+4 a
Iodine	^{131}I	beta, gamma	2.4 E-9 (vapour: 2.0 E-8)	high	yes	high	8.04 d
Iodine	^{123}I	gamma	6.4 E-11	high	yes	high	13,2 h
Iodine	^{125}I	gamma	1.4 E-9	high	yes	high	60,14 d
Cobalt	^{60}Co	gamma, beta	1.0 E-8	high	no	medium	5.27 a
Caesium	^{137}Cs	gamma, beta	9.7 E-9	high	no	medium	30.0 a
Strontium	^{90}Sr	beta	3.6 E-8	medium	no	medium	29.1 a
Technetium	^{99}mTc	gamma	1.9 E-11	high	no	low	6.02 h
Tallium	^{201}Tl	gamma	4.4 E-11	high	no	low	3.04 d
Iridium	^{192}Ir	beta, gamma	5.2 E-9	medium	no	low	74 d
Radium	^{226}Ra	alpha	3.5 E-6	low	no	medium	1600 a
Molybden	^{99}Mo	beta, gamma	1.1 E-9	high	no	high	66 h

Name		main radiation emitted	Toxicity (Inhalation) (eff. dose coeff. [Sv Bq^{-1}]*	Toxicity (external radiation) *	Volatility (at 20°C)	Water solubility	Physical half-life
Polonium	^{210}Po	alpha, gamma	1.1 E-6	low	yes	low	138 d

* Effective Dose coefficients: Values for adult persons were used.

Table 2-9: Availability of likely radiological agents

Name		Raw Material / Precursor	Source location
Americium	^{241}Am	smoke-detectors	research labs, smoke-detector-producers
Uranium	^{238}U	depleted Uranium, radioactive NPP waste (nuclear power plant)	mining, reprocessing plants and NPPs
Uranium	^{235}U	HEU, NPP fuel	NPP-fuel, nuclear weapon
Plutonium	^{238}Pu	thermoelectric generators, neutron sources	research labs
Plutonium	^{239}Pu	weapon-grade Pu	arsenals of nuclear weapons, NPP fuel
Iodine	^{131}I	sources available	hospitals, laboratories
Iodine	^{123}I	sources available	hospitals, laboratories
Iodine	^{125}I	sources available	hospitals, laboratories
Cobalt	^{60}Co	Single compact sources of ^{60}Co are readily available, fission product	hospitals, laboratories; important gamma ray source, extensively used as a tracer and a radio therapeutic agent
Caesium	^{137}Cs	as radiation sources readily available, fission product	hospitals, laboratories
Strontium	^{90}Sr	fission product, thermoelectric generators; radiation sources	nuclear reactors, hospitals (radiotherapy& diagnostics), industry
Technetium	^{99m}Tc	99Mo-sources	hospitals, laboratories
Tallium	^{201}Tl	sources available	hospitals, laboratories
Iridium	^{192}Ir	sources available	hospitals, laboratories
Radium	^{226}Ra	sources available	hospitals, laboratories
Molybden	^{99}Mo	technetium generators	hospitals, laboratories
Polonium	^{210}Po	thermoelectric generators, neutron sources	satellites, industry

2.5.4 Simulants and interferents

Due to their high toxicity, it is often necessary to conduct studies examining chemical agent behaviour using simulants with very similar physical and chemical characteristics but which are less harmful to humans. With respect to radiological agents, simulants are used in the context of training with dispersed (open) radionuclides where contamination and incorporation can take place. In such a context, often short-lived radionuclides are used instead of long-lived RN, because this reduces the problem of decontamination. Physical decay of short-lived RN leads to a disappearance of harmful radiation within a known time-span where after 7 half-lives radioactivity is reduced to one millionth of the original value.
Long-lived gamma-emitting radionuclides like typical fission products such as ^{137}Cs or ^{60}Co which are relevant in nuclear power plants (NPP) operations or accidents can be replaced for training purposes by ^{99m}Tecnetium. For beta-emitters like ^{90}Strontium, the short-lived ^{140}Lathanium is used as a simulant.

Interference is a relevant problem also for radiation detectors, where the presence of other radionuclides can have negative impact on the sensitivity or correctness of the detection of an instrument. In addition to problems caused by the raising of background due to other radionuclides present, there is the security-specific problem of the masking of harmful radionuclides like special nuclear material by less harmful medical radionuclides. For the prevention of nuclear smuggling nuclide identification is of highest importance, therefore the interference of two or more radionuclides has to be detected to avoid masking of security-relevant radionuclides like weapons grade plutonium (WGPu) or highly enriched Uranium (HEU). More expensive detectors with high resolution can be helpful in this context as well as additional use of neutron detectors.

2.5.5 Interference testing

Concerning the interference with ionizing radiation (elevated background); ANSI standards demand that detection instruments shall be able to identify the radionuclide of interest in the presence of an increased gamma-ray background from natural thorium (^{232}Th). For beta radiation, the instruments under test shall identify a radionuclide of interest when exposed to the photons emitted from a shielded pure beta-emitting radionuclide. The instrument is exposed to a shielded beta emitter such as (^{32}P or ^{90}Sr/^{90}Y). (ANSI 2006)

The complex gamma spectrum of a given radionuclide can overlap with the spectrum of the radionuclide of interest, hiding peaks relevant for the identification.
Critical combinations with a high risk of masking HEU are included in the testing procedure of IEC and ANSI standards for spectrometric detectors (see Table 2-10). Typical medical radionuclides include: ^{18}F, ^{67}Ga, ^{51}Cr, ^{75}Se, ^{89}Sr, ^{99}Mo, ^{99m}Tc, ^{103}Pd, ^{111}In, Iodine (^{123}I, ^{125}I, and ^{131}I), ^{153}Sm, ^{201}Tl, ^{133}Xe.

Table 2-10: Masking of SNM with other radionuclides

Standard	SPRD * ANSI N42.48	SPRD * IEC 62618	RID (radioisotope identifier) IEC 62327
Masking	**1 : 2 µGy/h;** e.g. ^{67}Ga : ^{54}Mn HEU : ^{67}Ga or HEU : ^{99m}Tc RGPu : ^{137}Cs **=>8/10 (positive alarms in 8 of 10 incidents)**	**1 : 2 µSv/h;** HEU : ^{99m}Tc WGPu : ^{131}I RGPu : ^{131}I **=>8/10** within **5 min;**	**background + 0,5 µSv/h** (± 30 %) ^{137}Cs + HEU ^{131}I + HEU ^{57}Co + HEU ^{133}Ba + RGPu **=>9/10** within 1 min

* **(spectrometric personal radiation detector)**

For the masking of special nuclear materials (like HEU = highly enriched Uranium, or reactor-grade Plutonium) several IEC standards for detection systems testing have included specific procedures (e.g. ANSI N42.48-2008: American National Standard Performance Requirements for Spectroscopic Personal Radiation Detectors (SPRDs) for Homeland Security) (chapter 6.10.4, p. 20).

"…The instrument shall provide an indication (e.g., the correct identification, "unknown," "unable to identify") when exposed to a radionuclide masked by another radionuclide that is not listed in the library or that has a much higher radiation intensity than the unmasked radionuclide.
[…] The test shall consist of ten trials for each source combination. The performance is acceptable when the instrument indicates that there may be a masking condition present in eight out of ten consecutive trials."

2.6 Specifics of explosive detection

Explosive detection is a non-destructive inspection process to determine whether there are explosive materials present. Explosive detection is commonly used at airports, ports, secure facilities, large event facilities, and for border control. The list below illustrates the most common applications of explosives detection.

- Screening of passengers
- Screening of hand-carried items
- Screening of checked baggage
- Screening of containerized cargo
- Screening of passenger vehicles
- Screening of mail
- Pre-incident search
- Post-incident analysis
- Protection of critical infrastructure

Each of these applications may require different technologies or the use of multiple technologies simultaneously. For example: screening of passengers can be done to find small amounts of explosives or to find threat items that have been concealed or both. This example leads to the discussion of the technical breakdown of explosives detection. Explosives detection can be broken down into two general categories: trace explosive detection and bulk detection. In the example given, the search for small amounts of explosives is covered under trace explosives detection and the search for concealed threat items under bulk detection. These two categories will be described below.

Trace explosives detection involves the chemical detection of explosives by collecting and analyzing microscopic amounts of explosives. The focus is not in finding the actual explosive rather it is focused on finding the residue or contamination that may be present from the assembly and/or transport of the explosive.

The early development of trace explosives detectors centred on the collection of the explosive vapour that may be present. This type of detection was hindered by the fact that most explosives have very low vapour pressure as shown in Figure 2-2. This means that only extremely small amounts of explosive vapour will be present at room temperatures for the majority of explosives. Therefore, only explosives with relatively high vapour pressures such as EGDN and TATP were able to be detected.

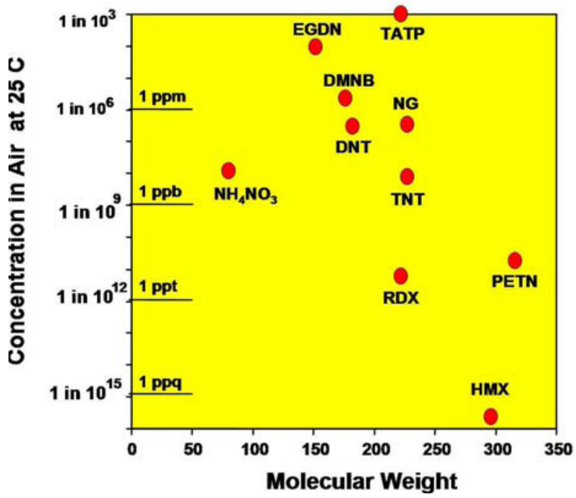

Figure 2-2: Explosives vapour pressures.
(Source: Thiesen et al. 2005)

To compensate for this initial shortcoming several things have taken place. First, the technologies involved have matured. Detection devices based on mass spectrometry (MS) have now been made small enough for field used. This gives the operator a powerful tool with excellent specificity and the capability of detecting amounts as small as a few femtograms (1×10^{-15} grams). Second, nitrogen based taggants with high vapour pressures have been added by manufactures to explosives to aid in their detection. The taggants however are added by legitimate manufacturers do not address the issues surrounding homemade explosives which lead to the last change in detection methodology. There has been a shift from purely vapour based detection to particulate based or a combined vapour/particulate based detection. Particulate detection is done by swabbing the suspect item and then analysing the swab. The downside of this type of detection is that the operator has to physically touch the suspect item which can be dangerous. Figure 2-3, below illustrates some of the available technologies for explosive trace detection.

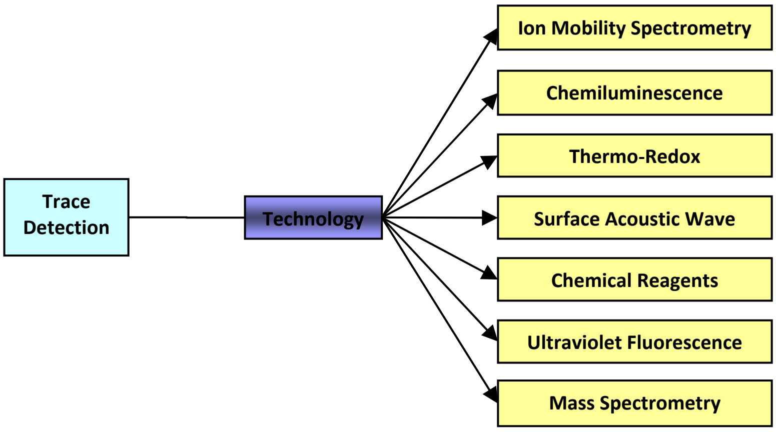

Figure 2-3: Trace detection technologies.
(Source: Thiesen et al. 2005)

Trace detection technologies

Ion Mobility Spectrometry (IMS)
IMS is the most common technology used in explosive trace detection. It is based on the speed in which ions move from the collector to the detector. The advantages of this technology are

- Scalability: from small and cheap handheld devices to large and expensive permanent portal entry points
- Ease of use: normally operated by one person after only a short period of training
- Sampling: both vapour and particle samples are supported

Disadvantages are:

- Nuclear source which is used as the ionizing agent can cause regulatory issues
- Differentiation: Ions of similar size can produce single broad peak instead of a distinct single peak. This is normally overcome by using a gas chromatographic (GC) column prior to the IMS.

Chemiluminescence (CL)
CL is based on the infrared light emitted from the exited nitrogen compounds found in many explosives.
Advantages:

- No radioactive materials
- Ease of use: normally operated by one person after only a short period of training
- Sampling: both vapour and particle samples are supported

Disadvantages:

- Detection: can only detect explosives that are either nitrogen based or have a nitrogen taggant.

- Specificity: CL cannot on its own determine the exact explosive present. This can be overcome by using a GC front end.

Thermo-Redox (TR)
Thermo-Redox technology is an electrochemical technique based on the thermal decomposition of explosive molecules and the subsequent reduction of NO2 groups. This technology has similar advantages and disadvantages as CL technology.

Surface Acoustic Wave (SAW)
Surface acoustic wave (SAW) detection of explosives materials is based on frequency changes that occur when materials are deposited on the SAW crystal surface (detector surface.). This technology is most often fielded with a GC front end. The main advantage of this technology is also its main disadvantage. SAW can detect the presence of other chemicals in addition to explosives, which makes explosive detection more difficult.

Chemical Reagent
This technology is based on colour changes that occur when chemical reagents are introduced to a sample. The method of collecting the sample is done by swiping a suspect surface with a specially prepared test paper. Vapour sampling is not possible.

The biggest advantages of this technology are its simplicity, ease of use, and low cost.
The main disadvantage is that the colour change has to be interpreted by the user.

Mass Spectrometry (MS)
MS is a mass filtering technique. Samples are ionized, passed through a filter, and then identified by the mass charge ratio. This technology is most often used with a GC front end as described earlier. This technology is a powerful laboratory technique which is now able to be used in field operations.

Advantages:

- Powerful analytic tool with excellent compound specificity
- No radioactive material

Disadvantages:

- Difficult to operate
- Size: Usually rather large devices weighing approx. 75 lbs
- Costly: Portable MS devices are expensive
- Time: The sampling analysis time can be relatively long

The second general category is bulk detection**. Bulk detection** involves the detection of a macroscopic mass (a visible amount) of explosives material. Bulk detection relies on the use of a radiation source to interrogate the material under inspection. Bulk detection can be further differentiated into two sub-categories: imaging and nuclear. Imaging is based on the physical appearance of the explosive device such as the wires, timers, detonators, and to a lesser degree the explosive material itself. Nuclear technology is based on the molecular properties of the explosive such as its Z number.

It should be noted that bulk detection is typically concerned with cargo. This is due to the x-ray and gamma ray sources used in this type of detection. These x-rays can have rather serious health consequences for humans should they be exposed. Recently however, there has been the development of low dose x-ray backscatter technology. In this technology the amount of radiation that is emitted during scanning is low enough to be used to screen passengers.

Some of the available technologies for bulk detection are shown in Figure 2-4.

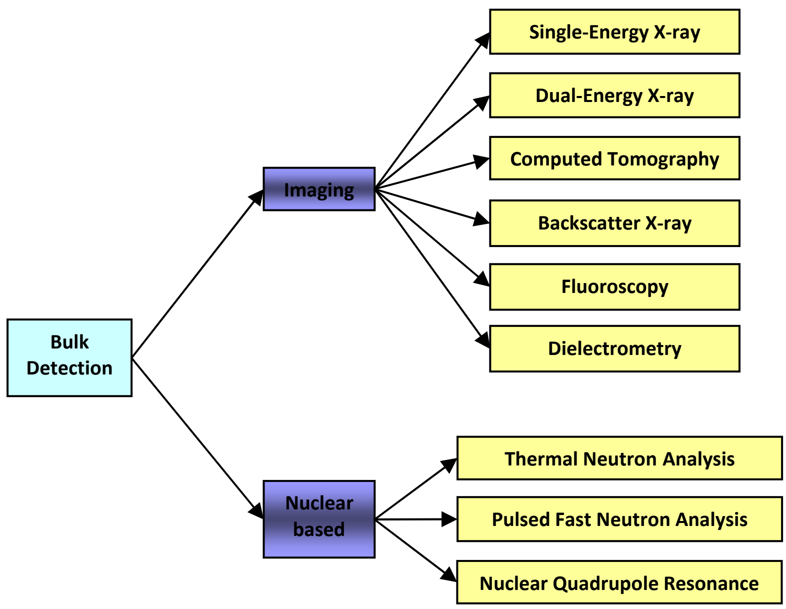

Figure 2-4: Bulk detection technologies.
(Source: Thiesen et al. 2005)

Bulk X-ray technologies

Single-Energy X-ray

This type of technology is typically used to screen cargo and vehicles. The image is simply indicates the level of absorption. Because of this, it is not possible to determine the actual explosive; rather the detection of the bomb parts is the goal.

Dual-Energy X-ray

In this technique, either a single x-ray source with two detectors, or two x-ray sources and a single detector are used. Two independent images are produced then computer processed into a final image. The final image has sufficient detail to determine objects by shape, and density. Artificial colours are often added to show inorganic and organic materials as well as suspect items.

Computed Tomography (CT)
CT is a technique that produces a three dimensional image from a series of two dimensional cross-sections. The advantage of this technology is that it can produce cross-sections of hidden items, material absorption coefficients can be determined directly from the item, and it can discriminate explosive like materials from others. The disadvantages are high cost, system complexity, and lowered throughput.

Backscatter X-ray Techniques
Backscatter is a technique that can determine the Z number of materials by the way the material scatter the input radiation. Backscatter systems are able to highlight organic materials better than the standard transmission x-ray image. Higher dose systems can be used to screen baggage while low dose systems can be used to screen personnel.

Fluoroscopy
Fluoroscopy is an x-ray imaging technique where transmitted radiation through an object is detected. A monitor can view a dynamic image or still images of the object. Fluoroscopic equipment is used typically as portable scanners for screening mail and small packages for explosive devices.

Dielectrometry
Dielectrometry, another imaging technique, uses a low-energy microwave field to irradiate objects. The dielectric and loss properties of the object are measured in the microwave field. The phase and magnitude of these field lines change depending on the dielectric properties of the object in the field. Dielectric property changes are due to various physical, chemical, or structural properties of the material.

The human body has a unique dielectric response (signature) and is different from any explosives signature. The system compares the dielectric of the object in the microwave field to known values (e.g., human body values) and can distinguish anomalous areas where the dielectric properties are different. The dielectric sensor is an anomaly detector that can detect anything of sufficient volume that is different from the human body or other material in question.

Bulk nuclear technologies

Thermal Neutron Activation (TNA) (Marshall & Oxley 2009)
Thermal neutron activation (sometimes also called thermal neutron analysis) is one of the first and most thoroughly investigated nuclear explosives detection technologies used. TNA is an explosives detection method based on the characteristic emission of gamma rays in the object of concern. A thermal neutron source interrogates a sample and the resulting distinctive gamma ray emission allows for an accurate measure of the nitrogen in the sample. The main advantage of this technology is that it can easily penetrate shielding that

could defect other x-ray technologies. The main disadvantages are: size, weight, cost and the presence of a radioactive source. This technology is use primarily at fixed installations such as for screening baggage at an airport.

Pulsed Fast Neutron Activation (PFNA)
Pulsed fast neutron activation (also called pulsed fast neutron analysis) is a technique where high energy neutrons are pulsed at the object of interest. The characteristic gamma rays emitted are detected, imaged and analyzed to determine what materials are present. The advantage of PFNA is its ability to penetrate metal objects in the cargo. Its main disadvantages are: size, weight, shielding requirements for scanning and its inability to penetrate hydrogenous cargo,.

Nuclear Quadrupole Resonance (NQR)
Nuclear quadrupole resonance (NQR) is an explosives detection method based on nitrogen quadrupole detection. A weak radio frequency (RF) signal is detected from the quadrupole nuclei present in the explosive material. Its advantages are high chemical specificity and the ability to detect very small amounts of certain explosives. The disadvantages are: only detects crystalline solids, it can be easily shielded, and it can be interfered with by AM band radio signals.

2.6.1 Typical explosive agents

Table 2-11 below presents the most common explosives. The last item in the table is TATP. This is an explosive of interest. First, it is a homemade explosive that is relatively easy to produce. Second, TATP is not nitrogen based making it more difficult to detect. Lastly, this explosive seems to be the explosive of choice for terrorists and insurgents and has been involved in numerous incidents over the last decade.

Table 2-11: Common explosives

Common Explosives			
Name	Type	Composition	Notes
Black Powder	Low Explosive	Salt peter/sulphur/charcoal	safety fuse, homemade, pipe bombs
Smokeless Powder	Low Explosive	Guncotton/ether/alcohol	Ammunition propellant, pipe bombs
Blasting Cap	Primary High Explosive	Lead Azide/Lead styphnate/RDX/PETN	used to detonate a main charge
Detonating Cord	Primary High Explosive	PETN	used to detonate main charges
Pentolite	Secondary High explosive Boosters	50% PETN,50% TNT	Provide detonation link between PHE and the main charge
RDX	Secondary High explosive Boosters	Cyclotrimethylene trinitramine $C_3H_6N_6O_6$	Provide detonation link between PHE and the main charge
PETN	Secondary High explosive Boosters	Pentaerythritol tetranitrate $C_5H_8N_4O_{12}$	Provide detonation link between PHE and the main charge: used to boost ammonium nitrate
Tetryl	Secondary High	$C_7H_5N_5O_8$	Provide detonation link between

Common Explosives			
Name	Type	Composition	Notes
	explosive Boosters		PHE and the main charge: most common military booster
Dynamite	Secondary high explosive main Charges	Nitroglycerin with wood pulp $C_3H_5N_3O_9$	Used in blasting operations. Relatively easy to obtain
Ammonia dynamite	Secondary high explosive main Charges	Nitroglycerin + EDGN + wood pulp	Used in blasting operations. More stable than straight dynamite
Gelatin dynamite	Secondary high explosive main Charges	Nitrocellulose + Nitroglycerin + wood pulp	Used in wet blasting applications
Military dynamite	Secondary high explosive main Charges	RDX + TNT + motor oil + cornstarch	Used for military blasting operations: substitute for straight dynamite due to its stability
Ammonium Nitrate	Secondary high explosive main Charges	$(NH_4)(NO_3)$	Commercial fertilizer and blasting compound
EGDN	Secondary high explosive main Charges	ammonium nitrate and nitroglycol	Used in blasting operations
ANFO	Secondary high explosive main Charges	ammonium nitrate + fuel oil	Commonly used as a homemade explosive. Has been used in numerous bombings
Kine-Pak	Secondary high explosive main Charges	ammonium nitrate and nitromethane	Two part explosive designed to replace dynamite
Kine-Stick	Secondary high explosive main Charges	ammonium nitrate and nitromethane	Two part explosive designed to replace dynamite
Astrolite	Secondary high explosive main Charges	ammonium nitrate and hydrazine	Liquid explosive used in blasting. Especially for blasting cracks, crevices or modified containers
TNT	Secondary high explosive main Charges	Trinitrotoluene $C_7H_5N_3O_6$	Most widely used military explosive. Used in artillery shells, aerial bombs, mortar rounds
Tetrytol	Secondary high explosive main Charges	70% tetryl and 30% TNT	Used as an alternative to TNT in military applications
Match heads	Improvised main charge explosive		Used as an improvised explosives. Typically in a pipe bomb
Potassium/Sodium Chlorate	Improvised main charge explosive		Used as an improvised explosives. Typically in a pipe bomb. Similar to 40%
TATP	HME	Hexmethylene triperoxide diamine	Used a home made primary high explosive, used in the Middle East by insurgents

(Source: Eiceman et al. 1999)

2.6.2 Interference testing

Interferents are non-explosive substances that exist in the environment where an explosive detector is being operated that can cause either false positive or false negative decisions. The mechanism by which a false negative decision is created is by desensitising the detector. Essentially, the interferents make the detector unable to recognize an existing explosive. A false positive decision is created when the interferent mimics an explosive compound closely enough to generate an alarm. One of the goals of operational testing is to determine the detection efficiency with respect to the effects of interferent compounds. There are several issues with this that need to be considered.

First, there are an enormous amount of possible interferents. It is obviously not possible to exhaustively test every possible interferent/explosive combination as the numbers of tests required would be prohibitively expensive in terms of time and money. Presented below is just a small sample of some compounds that are considered interferents to explosive detection. (Ellis-Steinborner, Johnson 2007)

- Polishers: shoe, car and furniture
- Cleaners/disinfectants such as: bleach, soap, vinyl cleaner
- Mothballs
- Deodorants
- Personal hygiene products: soap, nail polish remover, aftershave lotion, hair gel and hand cream
- Herbs and spices
- Automotive products: lubricants and cleaners
- Other chemicals: fertilizers, acetone, alcohol, solvents, insecticides

Second, interference testing is detector technology specific. Depending on a given technology a different type of interferent must be used. For example: if one is testing a chemical reagent kit, nitro-musk perfumes and nitro-methane solvents can be used as interferents. On the other hand, if one was testing an IMS based detector a broad range of interferents could be used so long as the size, charge and molecular weight are similar to the explosive compounds to be tested.

Finally, the interferents to be used are environment specific. There has to be an understanding of the intended use of the detector and the environment involved. For example: If the detector is to be used in the screening of passengers then interferents such as personal hygiene products would be likely candidates to be tested. However, if the detector is to be used in the screening of mail it is likely to require a different set of interferents.

At present, there is no consolidated understanding of the issues presented above. Much of the testing of interferents is done by experience and from literature available. Therefore, to have an effective operational evaluation of the effects of interferents it may be necessary to create a knowledge base. Within the knowledge base there should be a summary of the explosive detection technologies available, the possible interferents for each technology, and the possible employments of each technology. Then based on the aforementioned items a summary could be produced showing the interferent testing recommendations.

3 Operational testing – the concept

In Figure 3-1 below we see the typical timeline of system development. During the early stages of development when the capabilities that are required are changing and are being refined there exist Development Test and Evaluation (DT&E) programs. These programs are put in place to ensure that the performance goals are being met. The testing conducted in DT&E is done by the manufacturer internally. Following that, in the engineering manufacturing development through to initial production stages, there is the initial introduction of Operational Test and Evaluation (OT&E) program.
OT&E is formal testing conducted prior to the deployment of a system. It is designed to evaluate the effectiveness and suitability of the system with respect to its intended use. In this case, the manufacturer is testing the final design before it reaches full production. Additionally, some OT&E can be done at this stage by the potential customer during their acquisition phase. This is done particularly for large phased projects, where the customer wants to assess the ability of the system to meet the original needs as articulated and modified during earlier design phases. Normally, to ensure objectivity, this type of OT&E is conducted by a testing agency within the customer's organization that is independent from the acquiring agency. It should be noted that during the DT&E and the initial phase of OT&E, the testing is centred on the laboratory testing of the system.

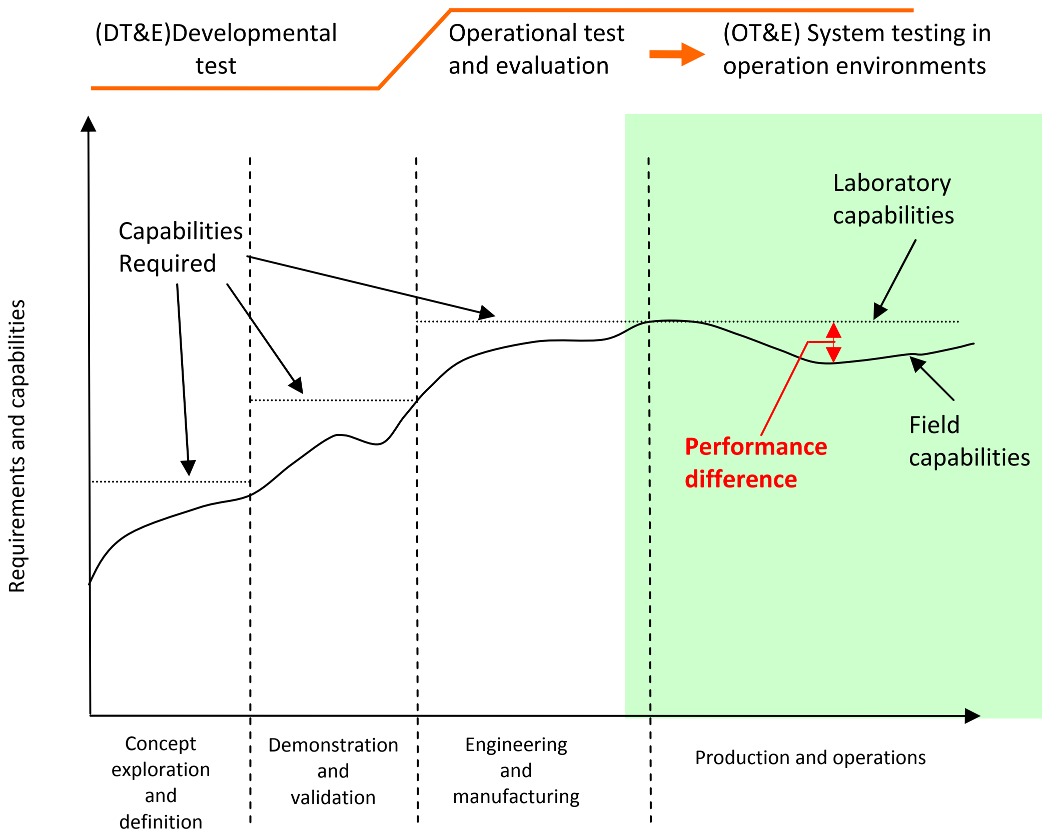

Figure 3-1: Testing and Evaluation during product life cycle.
(Source: adapted from Rapport, Balkcom, Stirrat, & Wilson 1996)

The goal of the operational testing framework (OTF) for CBRNE detection device is to redress what has been historically absent in the T&E programs: namely an OT&E program where the system is placed in operational environments and then tested. The phase of the life cycle effected by this program is highlighted in green in Figure 3-1. It is from the point where the system goes into full production up to the point when the system is retired. The purpose of the OTF is to investigate the "performance difference" which is highlighted in red in the figure. It is the difference between the laboratory capability of the system and the use-case capability determined in the field. The qualification and quantification of the "performance difference" as well as other reasons for this type of OT&E are alluded to below.

First, OT&E can be used to verify the claims made by the manufacturer but in a field environment. It is not intended to simply duplicate the laboratory testing where the testing is normally done under ideal conditions to determine the best-case values for the detector in a fixed environment. Operational testing is designed to determine the use-case values of a specific detector. More specifically, operational testing is designed to determine the operational performance of a specific detector while taking into account the environmental, operational placement, usability, and other affects that are present in the actual deployment of the system.

General performance measures to be determined could include (but aren't limited to):

- Specificity
- Selectivity
- Probability of detection p_d
- Confidence interval
- False positives/negatives
- Operational range (temperature, pressure, humidity, etc)

Second, there are numerous issues that are not normally evaluated in laboratory testing that will be addressed in OT&E. Some fall under the general heading of operational testing whereas others fall under the heading of human factors testing which is a subset of operational testing.

Operational tests:

- Operational placement
- Resistance to interferents
- Test of the user's manual

Human factors testing:

- Usability: How easy is the detector to use
- Operational interaction
- Throughput testing
- Affect of personal protective equipment on usage
- Decontamination

Parameters not tested but to be determined:

- Cost of procurement

- Cost of consumables
- Cost of maintenance
- Shelf life

Third, from the data gathered from what is noted above, it is possible to draw conclusions about a specific detector such as its suitability for specific application, climate range, operational placement issue, resistance to interference, etc.

Next, there is the benefit to the end-user community. Traditionally, testing has not focused on the end-user but rather has focused simply on the technical data. The output of the operational testing is always focused on the end-user community. From this testing it is possible to present the end-user with a consolidated and a comprehensive report that will facilitate their purchase and deployment of an appropriate detector. It will allow them to effectively compare detectors with an independent verification.

Finally, there is the potential to give feedback to the manufacturer regarding their detector. For example: the operational performance of their detector in comparison to the other detectors in the same class on the market. It is also possible to make note of areas of the performance of the detector that can be improved or to propose additional functionality.

3.1 Introduction to the elements of operational testing

In the following sub-sections: 3.2, 3.3, and 3.4 we will introduce three critical elements of our operational testing framework, scenarios, human factors testing and evaluation, and considerations for testing. First, subsection 3.1 introduces the scenarios. The scenarios are the cornerstone of the operational testing. They are carefully selected scenarios that represent situations that end-users could find themselves in and are based on incidents that have either occurred or are likely to occur in the future. In their current form they are rather general in nature and many of the details have been omitted. In future work, they will be much more detailed and will create an operational testing script that will frame the testing.
Next, Subsection 3.2 introduces Human Factors testing and evaluation (HFTE). HFTE is almost never covered in laboratory testing yet it may the most influential portion of operational testing for the end-users. In this subsection, we discuss a brief history of HFTE, a general structure for developing HFTE tests, and a general example from aviation security. Through the use of HFTE we will be able to answer the questions such as: how usable is the detector and what are the impacts on detector operations given the environment surrounding their use. Following that in subsection 3.3, we introduce operational testing of performance with human factors considerations. Within this subsection, we describe the several different test elements such as: throughput testing and user manual testing, which should be included in a comprehensive testing protocol. The elements presented are to be considered a starting point to operational testing and not an end point. This is the case for two obvious reasons: the elements only present reasons why to be included and basic considerations and not elaborate testing procedures and the list may not be complete and other elements can be added.

3.2 Scenario based operational testing

The scenario based tests can be used to evaluate if desirable capabilities are obtained with the detectors, training and methods available to the end-users. Test and evaluation of performance in an operational environment (described in subsection 3.4) is done to get specifications of detectors in an operational environment. In scenario based operational testing whole processes including detectors, methodology and human factors can be evaluated.

There are several objectives of the scenarios for WP3. First, the scenarios used should be derived from situations that can where special CBRNE capabilities are needed to solve them successfully. The scenarios must be designed to cover the operational conditions that the end-users (first responders) encounter. The test presented here consists often of a basic scenario that will set the stage for follow-on scenarios. Small adjustments can be made to test different detectors and aspects of the detection device and the operational implications. The actual agents that are used are not elaborated. The scenario can have numerous different agents that can be tested. However, in some cases the scenario itself is agent specific. In those cases, there are suggestions on suitable simulants or testing agents for the test.

The results from the tests should include an estimate of how well the trained unit or units could reach the goals of the test. In the analysis of how the test was carried out, end-users and decision-makers should be involved. It is important to find out how information and orders are interpreted and carried out in order to find suggestions for improvement. The answers may be found in malfunction detectors, lack of training or skill, bad communication or bad managing.

3.2.1 Selected chemical scenarios for operational testing

Scenario C1: Aerosol dispersion of low volatile compounds

The aim should be to detect low volatile chemicals as aerosol and gas in air, and as liquid droplets on the ground. The task should be to find the source and to determine a risk area. The source should produce aerosol droplets at a height of five to ten meters. Handheld, mobile and standoff detectors could be used to detect the aerosol and gas present in the air. Sampling and field analysis can be performed to determine the risk area.

> *Goal*: find the source and determine a risk area.
>
> *Trained*: Finding the source is a task for the police, but help could be required from other public authorities. Risk areas are often determined by fire brigades.
>
> *Material used*: A spraying device must be used, that produce an aerosol of the low volatile liquid. To be able to make risk areas, local weather must be measured or given as information to the team.
>
> *Detectors used*: Anything from detection papers to laboratory instruments could be used. The chosen detectors should be those that are likely to be at hand in a real event.

Results: If the teams find the source, it is a question of how much time it took and how much resources were spent. The determined risk area can be compared with a risk area derived from knowledge of the source and local weather condition. A good match will give a high score but since there are many parameters involved in the process, differences are to be expected. It is important to perform a thorough analysis of why and how the results turned out the way they did.

Scenario C2: Monitoring a fixed area

An open or confined area should be monitored in order to detect releases of medium to high volatile chemicals as gas and/or aerosol. The chemical could be released within the area, outside or above it. Handheld detectors, sensor networks and standoff detectors can be used in the test. In order to get a fast alert generic sensors can be used; for instance a photo ionization detector (PID). The warning should be verified by a detector capable of classifying or identifying the chemical. It is important to obtain a fast response, to detect threats and to be able to tell them apart from hoaxes or interferents.

Goal: is to give a fast response to be able to protect an area (building, football field, centre of infrastructure, etc). The information must at the same time be accurate and trustworthy in order to be reliable enough to make tough decisions.

Trained: teams with detection equipment and decision-makers.

Scale: the test can be carried out as separate tests for detection teams with or without decision-makers.

Material used: if simulants or test agents are used, gas can be produced from volatile liquid (by spraying devices, blasts of liquid canisters) or from gas cylinders.

Detectors used: a wide range of detection equipment can be used. If the test is focused on decision-making and command and control, simulation aids can be used instead of real detectors with simulants or testing agents. However, it is very important to use detectors that can provide an acceptable level of specificity.

Results: this test is very demanding. It demands fast response and high accuracy, which often require more than one kind of detector. Technical solutions should be combined with appropriate methodology and analytical skill to form the basis of good decision-making.

Scenario C3: Inspection of risk objects

There is an object (gas cylinder, gas tank, or other object) which is assumed to contain a toxic gas. The object may have a leak. The task is to monitor the object to be able to detect if and when gas is leaking from the object, and to determine which chemical it is. Big leaks can be determined by eye, but to find out which chemical is dispersed detectors are needed. Depending on the nature of the object handheld detectors, sensor networks, standoff detectors and remotely controlled detectors on unmanned vehicles (UGV/UAV) may be used.

Goal: monitoring an area around a risk object to detect leaks.

Typical user: first responders (fire fighters or police)

Scale: The location of the risk object can be inside a facility (shopping mall, airport, etc.), or in an urban or rural area.

Material used: from a gas cylinder to a gas tank. The gas can be compressed or condensed. Condensed gases give much larger dispersions.
Detectors used: intelligence is that there is a risk object. Detectors are used to obtain the source concentration, which is used to calculate a risk area.
Results: A fast response and proactive measures to minimize the effects of the gas dispersion should give a good score.

Scenario C4: Finding toxic liquids at checkpoints
Liquids should be scanned for toxic chemicals or precursors at a checkpoint. The liquids should be contained in bottles of different size and material. The bottles should contain ordinary liquids (perfume, shampoo, liquid soap, beverage, etc.), bulk chemicals of different concentration and mixtures of toxic chemicals and ordinary liquids. Important aspects are false alarm rate and throughput.

Goal: high throughput and low false alarm rate.
Trained: customs or police
Scale: the number of persons crossing the check-point should be enough to give statistically significant numbers of false positives and false negatives. If an accuracy of 99.9% is demanded, about 3,000 samples with illicit material are to be used.
Material used: ordinary product packaging should be put in bags, suitcases and coat pockets. The contents of some of the packaging should be exchanged with illegal chemicals. Simulants may be used instead of CWA and other toxic or expensive chemicals.
Detectors used: dedicated detection systems.
Results: throughput and false alarm rate should be compared between systems.

3.2.2 Selected biological scenarios for operational testing

Scenario B1: Suspect package
This scenario has been modified from CREATIF D.1.2 B-1.
A suspect postal package has been found in a postal office. The package has an unlikely sender's address, and the receiver is an important person in the government. Furthermore, the postal worker has dropped the package on a table resulting in fine dust coming out. The package is suspected to contain anthrax powder. The postal worker feels sick, but this could be the effect of fear. The building has been evacuated. First responders should go in to investigate the package and take samples for analysis. The first responders need two kinds of bio detectors:

1. A bio detector that is able to sniff the air in the room for anthrax spores that float around. This detector should be sensitive enough for low concentrations, able to respond quickly (near real time), and not give false alarm.
2. A bio detector (or rather bio-analyser) that can quickly analyse (on site) a sample taken from the package and produce a clear answer.

Scenario elements that influence a future test protocol (to be designed):

- Indoor, office
- Room temperature and humidity
- Narrow space, lots of surrounding equipment
- Air-conditioning, doors, drafts, etc
- Responders wear PPE

Scenario B2: biological aerosol release

The authorities have reason to believe there is a threat of a pathogenic bio-aerosol released during some major event where a large crowd of people are in an enclosed area. The threat is not serious enough to cancel the event, but still.... First responders are asked to install monitoring bio-detectors to raise the alarm if a suspect bio-aerosol is detected. The first responders need this kind of bio-detector:

- An automated, stand-alone air collector and bio-analyser that automatically sniffs the air and analyses it. As soon as something pathogenic is detected, the detector produces an alarm. The alarm triggers further reaction from the first responders.

Of course additional precautions need to be taken (evacuation plan, panic prevention, silent alarm, PPE ready, bio-analysers ready, ...), but again we focus on the detectors and what the consequences of this particular scenario are for an operational test procedure.

Scenario elements that influence a future test protocol (to be designed):

- Several types of area (theatre, sports arena, maybe indoor or (semi)outdoor, ...)
- Range of temperatures and humidity (indoor, outdoor, different seasons, ...)
- Large area, multiple detectors needed in several locations.
- Different wind speed and direction
- Many types of interferents possible (pollen in spring, sneezing people already having other infectious diseases, other types of dust and bio-aerosols, ...)

Scenario B3: Food contamination with a biological agent

Several people have fallen ill in a district of a major metropolitan area. The symptoms look like food poisoning. The scenario is like the Oregon salad bar poisoning by the religious cult of Bhagwan Shree Rajneesh in 1984. In this case the human has already served their purpose as a bio-detector, by becoming ill and thereby indicating the use of a pathogen. Hospital staff is already using bio-analysing equipment (clinical equipment) to determine the species of pathogen. First responders are not really needed here. Still, investigation teams go out to all restaurants and food producers in the area to look for the source.

Scenario elements that influence a future test protocol (to be designed):

- No need for very fast detection
- No need for PPE
- High throughput beneficial
- Detector (analyser) able to handle range of tough samples that may inhibit analysis

3.2.3 Selected radiological/nuclear scenarios for operational testing

Scenario RN1: Radioactive release via dirty bomb
This scenario has been modified from CREATIF D.1.2 RN-1
At morning rush hour a bomb explodes in a metro station causing immediate casualties and an unnoticed release of radioactive material. For a while the release of radioactive materials stays unnoticed so that the contamination spreads from the originating station to nearby stations and to trains. Some travellers are contaminated and transfer the contamination to their work place. A couple of hours afterwards, some first responders and metro travellers suffer from skin burns, headache and nausea. Some people go directly to hospital or their family doctor.

Scenario RN2: Radioactive release from a nuclear power plant
This scenario has been taken from CREATIF D.1.2 RN-2
A plane full of fuel and passengers is hijacked by terrorists. They take control of the plane. Soon afterwards the plane crashes into a nuclear power plant. A nuclear power plant has been extensively damaged. The reactor building and the cooling tower are both demolished. At present, there is thought to be a release of radioactive material from the damaged buildings, primarily the cooling tower. The situation exists that there could be a Chernobyl-like meltdown if actions aren't taken immediately.

3.2.4 Selected explosive scenarios for operational testing

Scenario E1: Vehicle borne improvised explosive device (VBIED)
This scenario has been taken from CREATIF D.1.2 E-1. It contains the original scenario with additional details to show the possible expansion of the scenario into test procedures.

At early morning, a large truck rammed through the security barrier at the main entrance to the "Palace Hotel" in a large city and crashed into the front of the building. Immediately following the initial impact the truck exploded. The force of the blast devastated the front of the building. The explosion also caused fires within the building which engulfed the entire building.

Rationale for the selected scenario
This scenario has been chosen for several reasons. First, this scenario is taken from a real world event: a suicide Vehicle Borne IED Attack on the Marriot Hotel, Islamabad, Pakistan, 20 September 2008. Second, the situation is relatively simple in nature and would not be prohibitively expensive to simulate. Finally, the basic scenario can be expanded to include a large number of sub scenarios that will be designed to test specific operational situations.

Expanded scenario details
This type of detail will be required to be developed further in later versions of the document. At present, these items are presented as a possible extension of the basic scenario towards a comprehensive testing protocol.

Detector types and technologies addressed by scenario

- Handheld explosives detectors (GC/IMS and GC/CL)
- Vehicle borne backscatter vans (backscatter x-ray)
- Vehicle borne X-ray scanners (medium energy dual source x-ray)

Considerations for the scenario

- Environmental conditions: e.g. temperature, time of day
- Space issues: In some situations the space available to make tests could be an issue. If the item under test in not readily available it would increase the difficulty in sampling.
- Personal protective equipment (PPE):
- Use of test facilitators (actors)
- Use of moulage kits

Outcomes foreseen

- Scanning/ imaging qualities
- Situational stress impacts
- Environmental impacts to detection
- Sensitivity of the detection device
- Affects of the PPE used
- Affects of the space issues
- Breadth of detection ability
- Usability of the detector during the scenario

Scenario test set up

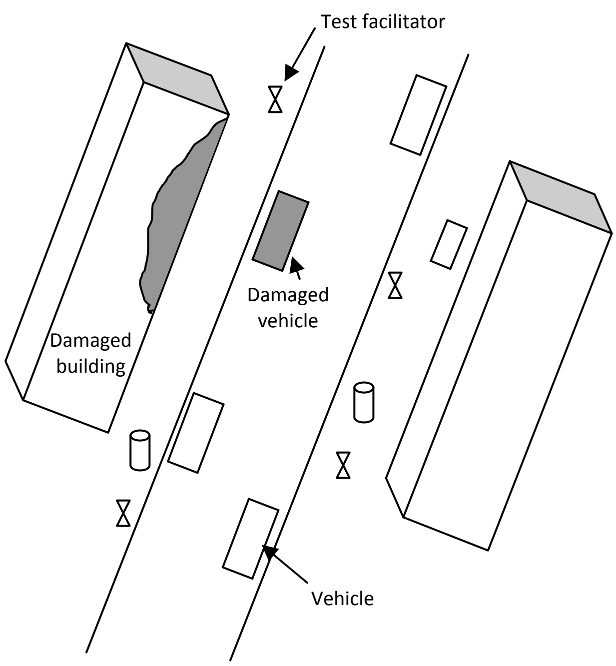

Figure 3-2: Explosive scenario E1 experimental setup

Extended scenario test procedures
As the test is developed separate sets of test procedures can be developed to test specific detector performance.

Scenario E2: Major event security screening checkpoint
This scenario has been modified from CREATIF D.1.2 Mixed-2. It currently only uses the explosives part of the original scenario.

A rock concert has been planned at the local sports stadium. The concert has been sold out for weeks and there are expected to be 60,000 people in attendance. A know terrorist organization know as the "we hate rock and roll group" has issued a threat that if the event takes place, there will be dire consequences. The group has alluded to the fact that they will use any means at their disposal to ensure that the event shouldn't take place including the use of CBRNE substances. It is known from their past actions that they are sophisticated enough to affectively plan, equip, and execute such and attack. Therefore, members of the local constabulary, fire brigade, Red Cross, and Military have been called to secure the event. At the main entrance to the stadium there has been setup a security checkpoint. They have at their disposal handheld, vehicle borne, and fixed detection equipment to cover a broad range of possible attacks. Furthermore, they have installed multiple standoff detectors on the outside as well as on the inside of the stadium.

As the event approaches its start, the group has once again issued a warning that if the event takes place, there will be an attack of some sort. It is the responsibility of the alerted groups to ensure that: no CBRNE devices are brought into the stadium, standoff detection of any attack outside the stadium can be detected remotely, and to mitigate the affects of any attack should one occur.

Scenario E3: Suspect Package
A suspect carry-on type bag has been left unattended in a waiting room of an airport. The bag has been placed between a trashcan and a bench. It has been reported that the bag has been there for quite some time (30mins) and the passengers in the area are becoming alarmed at the unattended bag. Attempts have been made to locate the owner of the bag via the airport public address system and up to this point no one has came forward to claim the bag. It is now considered, by the airport security personnel, to be a threat to the security of the passengers and the airport. The first responders have been notified that they should go to the location in question and investigate the bag and take all necessary measures to determine if it is a threat and if so, to act appropriately.

Rationale for the selected scenario
This scenario has been chosen for several reasons. First, it is a situation that is often faced by first responders. Given the amount of air travel, there is a distinct possibility that you will be in an airport when a situation happens like this. Second, is simplicity: this situation is not very elaborate and doesn't take a lot of materials to setup properly. Finally, the basic scenario can be expanded to include a large number of sub scenarios that will be designed to test specific operational situations.

Scenario E4: Passenger screening

At a major metropolitan airport people are waiting in line for their screening before boarding the plane. The people themselves are being screened for any device that may be hidden on their person. Their bags are being processed through a scanning device and are randomly being inspected for any dangerous trace elements.

Rationale for the selected scenario

Most scenarios focus on a terrorist attacks, a natural disasters, or industrial accidents. These situations are only part of the operations that are carried out using CBRNE detection devices. Every day, millions of people are travelling by air and are required to be screened for anything that may be dangerous. Additionally, tons of cargo are being shipped along with the passengers and also require proper screening.

3.3 Introduction to human factors testing and evaluation

Definition of human factors

Human Factors, is a discipline of study that deals with human-machine interface. Human Factors deals with the psychological, social, physical, biological, and safety characteristics of a user and the system the user is in. (Adams 2010)

Definition of human factors testing and evaluation

Human factors testing and evaluation (HFTE), is a set of methodologies to characterize, measure, assess, and evaluate the technical merit and operational effectiveness and suitability of any human-system interface. (O'brien, Charlton 2002)

3.3.1 Historical background

The birth of human factors testing can be traced back to the very beginning of recorded history. Much of its history can be linked to the development of improved military weapons. This can be attributed to the fact that the need for improved military weapons was the driving force behind technology and that for the majority of history domestic applications of technology lagged behind.

The earliest application of human factors testing was more or less done by trial and error and was focused on fitting the man to the machine rather than the converse. If the human didn't fit the machine then the human, not the machine, was replaced. Later, as the machines became ever more sophisticated the focused shifted to the complex interaction of the human and the machine. Shortly after the turn of the 20th century, Taylorism, or the scientific study of the worker, emerged as a means to increase the efficiency of humans in the workplace. (O'brien, Charlton 2002)

During the period from 1914 – 1945, the foundation of modern HFTE was laid. The driving force behind the boom in research was the emergence of aircraft in warfare and the automobile for the private sector. A great deal of research was done regarding the impact of human intelligence, special aptitude testing, test and measurement methods, development of training aids, human perception, motor behaviour, and complex reaction times just to name a few. Much of this research was conducted under the branch of psychology called behaviourism as HFTE wasn't considered its own discipline at the time.

Recently, there has been the development of a new theoretical basis for HFTE which is based on Russian psychology. This basis emphasizes a very subjectivist viewpoint in such features as the importance of the individual's goals in information processing; images in perception; the nature of the goal as not necessarily fixed but as determined by the human functions; and a highly molecular measurement technique related to time and motion methods in industrial engineering (O'brien, Charlton 2002).

3.3.2 Application to CBRNE detection equipment testing

The current application of human factors testing and evaluation is focused on the system development and is an internal activity of the product developer. It is applied from concept exploration all the way to production and deployment. The human is placed at the centre of design activities and then the system is designed around them. The focus is to maximize the synergy between the operator and the machine and is usually done long before the system ever makes it to production.

In our case, the situation is quite different. First, the CBRNE detectors to be tested have already been designed and have made it to market. Second, the developer of the detection system is not a member of the testing team. Therefore, our human factors test and evaluation plan will be used as an evaluation tool for third parties, in particular, the end-user community who will actually be using the device. The goal is to place the CBRNE detector in a realistic operational environment, conduct operations, and make an assessment based on a standardized rating scheme to be developed.

3.3.3 Human factors testing and evaluation – A starting point

The SITE approach shown below in Figure 3-3: The SITE Structure is an attempt to support the design of human factors test and the interpretation of test results by presenting human factors test issues within a context of situation, individual, task, and effect attributes. (O'brien, Charlton 2002)

Situation What are the relevant elements in the environment, stimuli, setting events, system functions, or goals?	**Individual** Who is using the equipment or operating the system? What is their experience, training, skills, and momentary cognitive states?	**Task** How is the equipment being used and what behaviours are occasioned?	**Effect** Success or failure? Satisfaction or disappointment?

Figure 3-3: The SITE Structure
(Source: O'brien, Charlton 2002)

Situation category
Essentially, this is the environment that the operator and the device are to be used. In the case of CBRNE detection device testing the environment is created through the use of scenarios.

Some elements to be considered could include but aren't limited to:
- Hardware
- Software
- Environment (time of day, temperature, noise levels)
- Manuals
- Training
- Staffing levels
- Allocation of functions
- Task design

Individual category
As the name implies this category focuses on the attributes of the operator. Human Factors Testing is the assessment of the system and the individual is a critical element therein.

Some of the attributes to be considered are:
- Physical fatigue
- Workload
- Skill level of the operator

Task category
This category specifies what the operator should be doing with the CBRNE detection device.

It could include the following elements:
- Elemental measurements (taking a swab of a suspect liquid)
- User control action such as calibration
- Clearing an alarm

Effect category
In this category is where the evaluation of the first three categories takes place.

Some of the outputs from this category can be:

- Pass/fail
- Satisfaction/dissatisfaction
- Time to start up
- Probability of detection P_d

The SITE mnemonic is the most basic way to look at human factors testing. It is designed to put the test designer in the frame of mind that the system performance is only important when it includes all of the elements, situation, individual, task, and effect. It also creates a structure for selecting and employing a comprehensive test suite.

Test planning
SITE should be used to aid in the creation of a complete test suit. It is a tool to help organize the effort of the test designer. It also aids in evaluation of the completeness of the test suite.

The design steps:

1. It is recommended to start with the effect category. Determine which outcomes and performance metrics are the most important to be tested.
2. Create a list of all relevant user tasks.
3. Determine what operator characteristics are to be measured.
4. Finally, determine the situational measures to be included in the test. In the case of this document, the scenarios will be the basis for the situation and will be elaborated over time to include all relevant issues.

3.3.4 Human factors testing example

What is presented below is an example of the first stages of development of a human factors testing protocol. It is an example taken from the aviation industry. The focus of the example is on developing human factors testing for bulk and trace explosives detection within the commercial aviation sector.

Figure 3-4, illustrates at a high-level the situation surrounding aviation security. The elements in yellow are the situation category of the SITE mnemonic. The blue element is the element that requires testing. Essentially, the blue element is the effect category of SITE.

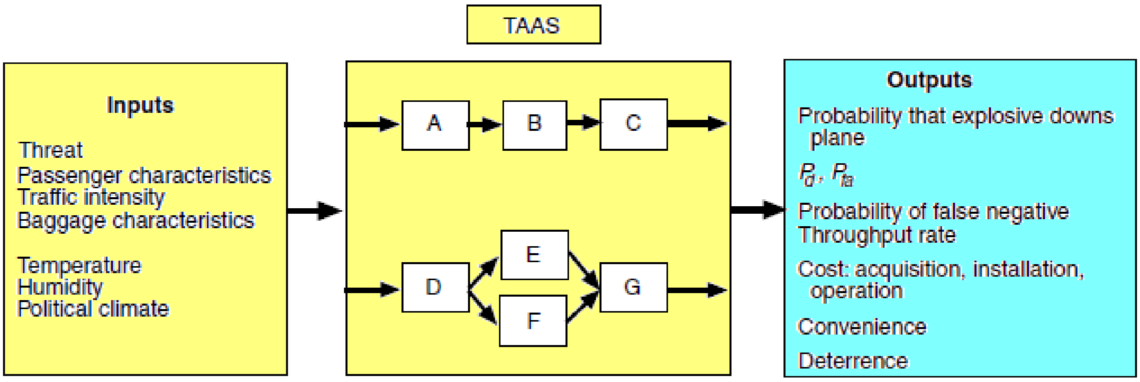

Figure 3-4: High-level Total Architecture for Aviation Security.
(Source: Committee on Commercial Aviation Security Panel on Assessment of Technologies Deployed to Improve Aviation Security, 1999)

Once a high level understanding of aviation security has been achieved, it is then possible to move onto an elaboration of the elements of the test.
Figure 3-5 is a more detailed look at the Total Architecture for Aviation Security (TAAS). It illustrates the situation surrounding the screening of baggage in a commercial aviation setting. Within the figure the element that generates the outputs from the first figure is again highlighted in blue to show their placement within the overall system.

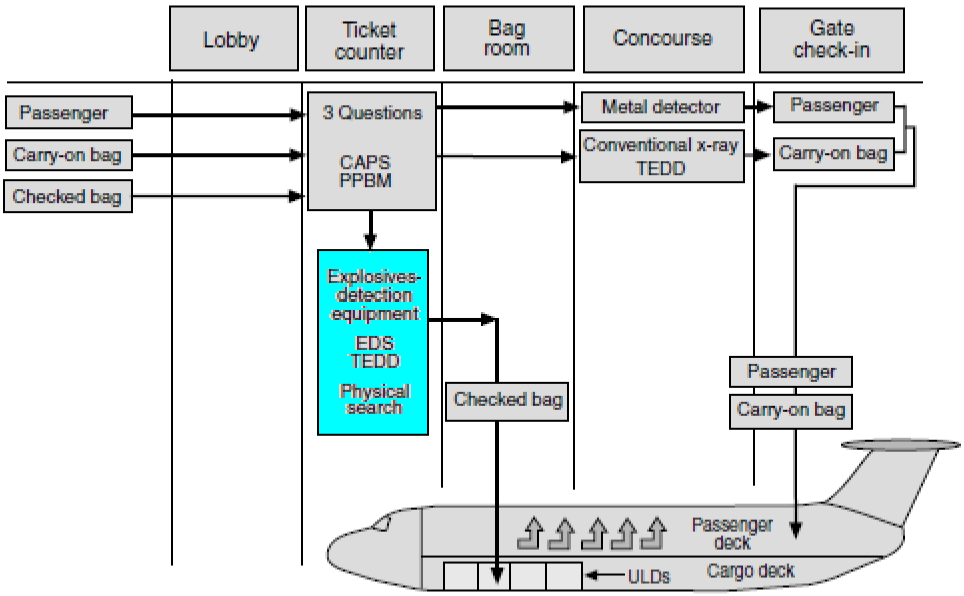

Figure 3-5: Total Architecture for Aviation Security.
(Source: Committee on Commercial Aviation Security Panel on Assessment of Technologies Deployed to Improve Aviation Security, 1999)

Figure 3-6 shows only one component in the overall TAAS to be tested. This component is linked to other components by how bags arrive for screening and by the alarm-resolution procedures. For example, if a TAAS configuration has two EDS in series with alarms on the first EDS resolved by the second, the human decision in the first EDS may not be critical. If noncertified bulk explosives-detection equipment is used that does not have image display capability but uses a go/no-go indicator, the operator is not involved in determining if there is an alarm but is involved in resolving it.

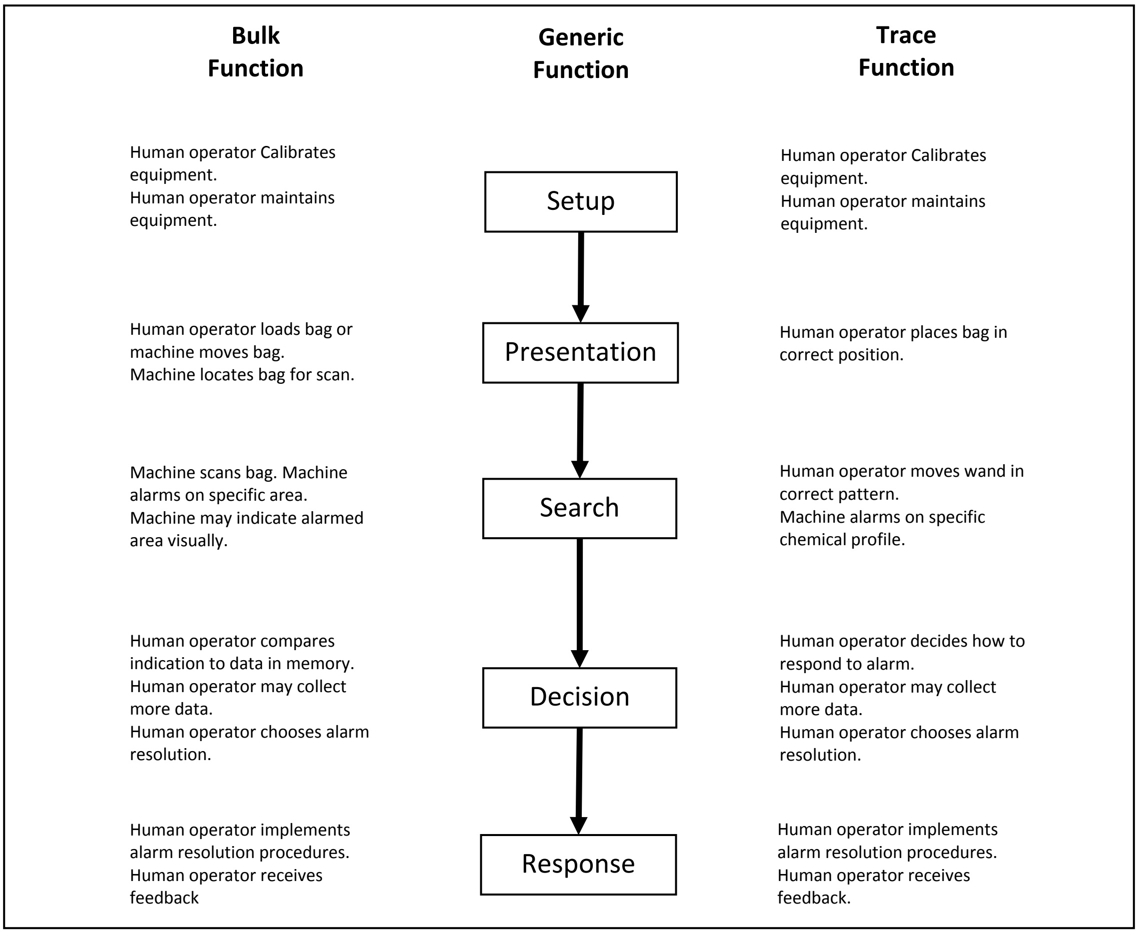

Figure 3-6: Role of the human operator in explosives detection.
(Source: Committee on Commercial Aviation Security Panel on Assessment of Technologies Deployed to Improve Aviation Security, 1999)

Next, Table 3-1 resolves the situation further. It presents a rather detailed description of the factors that affect the operator and systems performance. From this table it is now possible to start creating actual test procedures. For example: within the setup block there is a reference to the calibration of the device. The test procedures would describe each of the calibration steps, the operator interaction, and the observations from the test.

Table 3-1: Factors That Affect Operator and System Performance

Function	Task	Operator	Machine	Environment
Setup	1. Calibration procedures 2. Maintenance procedures 3. Time available for tasks	1. Ability to follow procedures accurately 2. Training (quality and timeliness) for calibration and maintenance	1. Operator interface for calibration 2. Operator interface for maintenance	1. Management support of equipment calibration and maintenance 2. Location of equipment 3. Availability of equipment operating procedures and other job aids
Presentation	1. Baggage selection	1. Training	1. Physical layout of equipment	1. Management control over baggage selected 2. Perceived and actual passenger pressure
Search	1. Defined wand search pattern	1. Training (quality and timeliness) for search pattern 2. Operator dexterity	1. Human interface (e.g., wand, alarm indicator)	1. Management support to ensure procedures are followed 2. Perceived and actual passenger pressure
Decision	1. *Pd* 2. *Pfa* 3. Time available	1. Knowledge of threats 2. Knowledge of potential false-alarm items 3. Experience, overall and recent 4. Ability to make a decision 5. Resistance to passenger pressure	1. Operator interface to display design 2. Operator interface to acquire additional information	1. Management support for following correct decision procedures 2. Perceived and actual passenger pressure
Response	1. Alarm-resolution procedures 2. Management provision of feedback	1. Knowledge of alarm-resolution procedures 2. Resistance to passenger pressure	1. Interface to other systems	1. Management support for alarm-resolution procedures 2. Perceived and actual passenger pressure

(Source: Committee on Commercial Aviation Security Panel on Assessment of Technologies Deployed to Improve Aviation Security, 1999

3.4 *Test and evaluation of performance in an operational environment with human factor considerations*

3.4.1 General performance testing

Performance data obtained from laboratory testing are used to determine optimal performance in a controlled environment. They are focused on the technical capabilities of the CBRNE detector and are considered upper bounds of performance. These measures are not to be considered the performance in the field. Therefore it is prudent to include testing for the general performance of the detector in operational conditions.

Some issues to be considered are but not limited to:

- Specificity
- Selectivity
- Probability of detection p_d
- Confidence interval
- False positives/negatives
- Operational range (temperature, pressure, humidity, etc)

3.4.2 Detector Usability

In laboratory testing there is typically no consideration of usability. A detector could have the highest level of specificity and selectivity in the laboratory but if the device is large, unwieldy, with fragile or ill placed controls, or a small or dim display it is unlikely to be chosen as a field device. Therefore it is prudent to explore the issues surrounding usability of the detector in the field.

The list below is a sample of some of the issues that should be considered.

Software

- Software packages used on the detector
- Proprietary software
- Easy of use
- Updatability

Hardware

- Ergonomics of the hardware

Displays

If the detector has a display, the following are some issues to explore

- Luminosity of the display (can it be easily seen in low light situations)
- Angles at which the display can be seen clearly
- Size of the fonts used
- Impact on the usability of the display if the user is wearing personal protective equipment

Controls

- Placement of controls

- Spacing of controls (spacing to avoid accidental actuation)
- Ruggedness of controls
- Type of controls (pushbutton, dials, or toggle switches)

Portability
Size and weight are less of a concern for detectors that are used in fixed installations or are desktop applications. In this case the operator will not have to physically carry the detector. However, for handheld or man portable detectors size and weight can have a significant impact on usability. The operator will have to carry the detector to conduct his operations possibly for extended periods of time. The longer the operator has to carry the detector the more important these factors become. Therefore, inclusion of testing with respect to the impacts of size and weight are warranted.

- Physical dimensions of the detector
- Unencumbered use
- Weight of the detector (upper bounds of handheld and portable detectors)

Robustness
Robustness is a measure of how rugged the system design is for transportation and field use. Furthermore, the system may be used in environmentally hostile conditions, which it must be able to withstand with no significant degradation in performance. (Ellis-Steinborner, Johnson 2007) Some points to be considered are:

- Detector packaging for transportation
- Recommended operating conditions
- Mechanical shock susceptibility
- Performance degradation due to normal handling in operational conditions
- Ability to switch modes of sampling if applicable

Power requirements
The power requirements of a CBRNE detector can have a significant impact on operations in the field. If for example the detector is to be used in remote locations where there is no access to electrical mains power or there is no availability of replacement batteries, the power needs can be a limiting factor in the detector deployment.

Issues to be investigated include:

- Power source: mains power or battery operated
    - 110V or 240V, or dual voltage source
- Time to charge batteries (if device is battery operated)
- Time of operation under normal conditions (time to fully discharge batteries)
- Type of batteries (common or detector specific)
- Availability and cost of batteries
- Affects of temperature and humidity on battery life

3.4.3 Evaluation of the user's manual

As with any product, there should be a user's manual. A user's manual is created and supplied by the manufacturer to the procurer upon receipt of the product. It is typically written by the manufacturer's technical writer but is presented in a fashion that keeps non-technical persons in mind. It is often written using as little jargon as possible and avoiding difficult technical issues. The purpose of the user's manual is to provide the customer with enough information to install, operate, troubleshoot, and maintain the product. It also provides information on the application of the product, background data, and should provide contact information for after sales customer support.

In practice, there is often little or no operator training. This can happen when the product may be procured by one department while the operators and in a different department. Additionally, the operator may not use the product daily and their skills in using it can diminish over time. In these cases the user's manual can be the only source of information for the operator. They will rely on the information contained therein to be able to operate the product. Therefore, it is critical that the user's manual be comprehensive and clear. The focus of operational testing with respect to the user's manual is focused on assessing the aforementioned qualities.

A related issue to the user's manual is that of customer service or after sales services that are provided by the manufacturer or vendor. Listed below are some items that need to be evaluated. The list is not comprehensive but is supplied as a starting point.

- Completeness: does it have the relevant sections
    - Introduction
    - System description
    - Product applications
    - Troubleshooting information
    - Maintenance information
    - Customer service contact information

- Correctness
    - Does the manual contain errors

- Ease of use
    - Topics clearly differentiated
    - Written on a level appropriate for the audience
    - Indexing (topic and sub-topic)

- Updatable
    - If there are updates, additions, or corrections can they be implemented

- Support
    - Web version available
    - Frequently asked questions
    - Electronic version (searchable)
    - Customer service support

- Instructions: typically there will be instructions for issues such as operational placement, setup, start-up, operation under normal conditions, error resolution and the like. These will need to be evaluated for completeness, correctness, and ease of use.

3.4.4 Operational interaction

Operational interaction is focused on the impact of the situation on the effective of the use of a CBRNE detector. Operational interaction can be divided into two general categories: incident response and screening.

In incident response a CBRNE incident has either occurred or a threat has been conveyed in some way. In this case, the first responders could enter into a highly chaotic and stressful situation and be called upon to conduct numerous activities on site including: searching for a CBRNE threat, determining which CBRNE agent has been released, and determining the extent of the contamination. All of these while they still might be tasked with providing first aid or decontamination.

Therefore it is prudent to assess the impact of the following (not a complete list):

- Situational stress
  - Injured and dead on the scene
  - Threat level: e.g. a highly toxic CWA versus a less toxic TIC.
  - The CBRNE threat that may still exist (pre-incident).
  - Weather
- Sleep deprivation: incidents may happen any time of the day
- Interaction with the people on-site while attempting to take samples.

Obviously, it is not possible to actually detonate an explosive, release a CWA, or inflict injuries for the sake of testing. However it is possible through the use of scenarios, mock ups, moulage kits (kits designed to simulate injuries) and test facilitators (actors to take the simulate individuals that might be on-site), to create a situation that closely approximates an actual situation.

The second general category is screening. An example of this would be an airport screener. While this type of operational interaction is usually less stressful than incident response there remains an interest in how the testing for CBRNE threats can be impacted by this situation. Some items that should be considered for testing are:

- Interaction with the individuals or cargo being screened
  - Having to physically touch the individual or item to be searched.
  - The individual speaks to the inspector
- Possible sources of interference: aftershave, perfumes, deodorants, alcohol
- The impact of the amount of time screening or monitoring.
  - 2 hour shifts versus 8 hour shifts
- Time of day: the impact of shift work
- Stress related to finding an threat material
  - Alarm resolution

3.4.5 Throughput testing

Throughput is an often cited characteristic of a CBRNE detector. In fact, in several applications such baggage, passenger, and container screening this may be the limiting characteristic. The throughput number presented by the manufacturer is often the number that has been obtained during certification of the device. This number almost certainly does not represent the actual throughput rate that is achievable in the field. Therefore, the throughput rate presented should be considered only the upper bound of performance not an accurate estimate of system performance.

There are several reasons for this disparity that need to be explored in operational testing.

- The time for alarm resolution should be included into the throughput rate. It has been shown in studies conducted by the U.S. Federal Aviation Administration that alarm resolution is the limiting factor in throughput rates.
- The impact of varying flow rates of items to be inspected needs to be explored.
- The impact operational placement of the detection device.
- Start up and warm up times needs to be considered.
- The human factors issues such as:
    - Experience and motivation of the inspectors
    - Staffing (length of the shifts, times of operation)
    - Situation stress of the inspectors
    - Skills maintenance of the inspectors

3.4.6 Personal protective equipment in operational testing

Personal protective equipment (PPE) shall mean any device or appliance designed to be worn or held by an individual for protection against one or more health and safety hazards. (EU Commission 1989). PPE must be worn whenever the wearer faces potential hazards arising from exposure to CBRNE hazards. Some examples of activities that may require the use of PPE are listed below:

- Activities before an incident
    - Hazard/threat mitigation: prevention of a release
    - Screening

- Activities during an incident
    - Emergency rescue: removing injured and or contaminated individuals
    - Site survey: investigation of the site during the incident

- Activities after an incident
    - Decontamination activities
    - Monitoring and supervision
    - Site survey: investigation following the incident to determine the exact cause of the incident

It is not the intention of this document to test the PPE itself but rather to test the human factors surrounding the use of the CBRNE detection device while using PPE. It is desired to determine what affects the PPE have on the usability of the device under test. There are several steps that need to occur to ensure the inclusion of PPE testing.

1. **Agree on a class of protection based on the different threats: chemical, biological, radiological/nuclear, and explosives.**

One such publicly available standard is that of NFPA 1994, Standard on Protective Ensembles for First Responders to CBRN Terrorism Incidents, 2007 Edition. Ensembles, boots, and gloves are certified to an NFPA standard by either the Safety Equipment Institute (SEI) or the Underwriters Laboratories Inc. (UL). SEI's certification programs are accredited by the American National Standards Institute (ANSI) in accordance with the standard, ISO Guide 65, General Requirements for Bodies Operating Product Certification Systems. Table 3-2 shows a comparison of the 3 NFPA classes.

Table 3-2: Comparison of NFPA 1994 Class 1, Class 2, and Class 3

NFPA 1994 Standard			
Characteristics	**Class 1***	**Class 2**	**Class 3**
Ensemble Configuration	Full-body, totally encapsulated suit with gloves and footwear	Full-body, encapsulating or non-encapsulating suit with gloves and footwear	Full-body, encapsulating or non-encapsulating suit with gloves and boots
CB Level of Protection	Highest	Intermediate	Minimum
Respiratory Protection	CBRN Self-contained breathing apparatus (SCBA)	CBRN SCBA	CBRN SCBA or an APR with appropriate filter canister or cartridge
Environment	Chemical or biological threat is unknown, the concentration is unknown, and the toxicity is not verified	Concentration of the hazard is immediately dangerous to life and health (IDLH) levels	Concentration of the hazard is at or below the short-term exposure limit (STEL)
Contamination Form	Gas, vapour, aerosols, liquids, or particulates	Limited exposure to gases vapours, liquid droplets, and splash	Liquid droplets and liquid splash
Skin Contact	Not permitted	Not probable	Not likely or not expected
Persistency	High	Moderate	Low
Proximity to Release	Close to the point of release both in time and distance	Separated from the point of release by either time or distance	Separated from the point of release by both time and distance

(Source: Fatah 2007c)

***Requirements for NFPA 1994 Class 1 ensembles have been incorporated into NFPA 1991 (2005 Edition) standards.**

A second standard has been created within the European Union. It is a more general standard considering all types of PPE and is not focused solely on the application of PPE in a CBRNE environment. It classifies PPE equipment as follows:

PPE classified as category I (simple design PPE) (EU Commission 1989)

PPE of simple design where the designer assumes the user can himself assess the level of protection provided against the minimal risks concerned the effects of which, when they are gradual, can be safely identified by the user in good time.

PPE classified as category II
This category shall cover all PPE not mentioned under categories I and III.

PPE classified as category III (complex design PPE)
PPE of complex design intended to protect against mortal danger or against dangers that may seriously and irreversibly harm the health, the immediate effects of which the designer assumes the user cannot identify in sufficient time.

2. Agree on a specific set of PPE to be used in testing.
Once agreement has been made regarding which standard is to be used it may be advantageous to specify several specific sets of PPE of each class that can be used in the operational testing. Standardization of the PPE used in testing is required to be able to produce comparable results from one test centre to the next. The PPE chosen for testing is not intended to replace the PPE used by specific organizations.

3. Inclusion of specific PPE testing in the test protocols.
The following list is not comprehensive but does illustrate some issue to be addressed in the testing:

Ensemble
- Weight
- Dexterity (e.g. impairment of body movement)
- Visual acuity/visibility

Gloves
- Dexterity (e.g. impairment of finger movement)

Mask
- Communications
- Hearing
- Field of view

3.4.7 Inclusion of decontamination testing within operational testing

Decontamination refers to means that reduce the hazard of a contaminant. There are two basic methods of decontamination, physical removal and neutralization. Physical removal involves mechanical action with techniques such as gentle friction with a soft cloth or sponge, blotting, and washing. Neutralization involves methods and/or materials to counteract the harmful effects of the contaminant (Lake 2008).

The CBRNE environment is an extremely dangerous one. The materials involved pose dire health consequences to humans. The instruments used to detect these materials will invariably be exposed to these materials. If they are not decontaminated properly the detectors designed to warn and protect will serve to cause injury. Therefore, as part of a comprehensive operational test protocol, it is necessary to test the decontaminability of the CBRNE detector. The decontamination protocols may be included in the user's manual and will likely be device and threat specific. Some issues to be considered when creating a decontamination test protocol are listed below:

- Is it necessary to decontaminate the detection device
- Is it possible to decontaminate the detection device
- Time to decontaminate
- Complexity of the decontamination activities
- Possible damage or shortening of detection device service life
- Cost of materials used to decontaminate detection device

3.4.8 Costs of operations

The items presented in this section are not items that can be tested in the traditional sense. These are items that are associated with the cost of operating a given detector. They can however be deduced during the testing program. Procurement cost is a one time cost that can be obtained from the manufacturer. The other costs can be obtained as the testing of a given detector progresses by logging the consumables used and the maintenance and calibration requirements. The last two items are a bit more difficult as they imply a longer testing period that may not be possible.

- Cost of procurement
- Cost of consumables
- Cost of maintenance
- Cost of calibration
- Shelf life
- Operational life

4 Evaluation protocols – Performance metrics

4.1 Introduction

One important issue surrounding operational testing is the choice of a rating scheme that will be used to qualify the results of the testing. Each characteristic of the CBRNE detection device needs to have some agreed upon manner in which to qualify them. Below are listed a few potential rating schemes that can be used for standardized testing. The schemes are listed from the least detailed to the most detailed. All of the schemes may have some applicability depending on the resolution required to fully qualify the characteristic.

These ratings schemes are not intended to eliminate or supersede the specification and data sheets supplied by the manufacturer but are intended to be used by the independent testing facility to more easily and clearly rate any given characteristic. The rating schemes are also designed to allow the procurers and operators to make a more valid side-by-side comparison of detection equipment without having to be an expert in the technical details.

Additionally, some of the details of operational testing are not hard science. They are not measured necessarily by exact numbers. Some characteristics are more qualitative in nature. These rating schemes may be more applicable for such qualitative ratings.

Below is presented four rating schemes that could potentially be used for the testing of CBRNE detection equipment. By no means is this list exhaustive but it does show some potential rating schemes. There are also example applications of each scheme described below the scheme.

4.2 Rating schemes

Sample rating scheme 1

This is the most simple of the rating schemes. It is a common rating scheme used in the private and public sectors to give decision makers a very quick assessment of the capabilities. It has only three ratings red, yellow, and green.

Table 4-1: Sample rating scheme 1

Sample Rating Scheme 1	
Green	Fully Capable
Yellow	Capable with limitations
Red	Failure/No Capability

Table 4-2 shown below illustrates one possible application of sample rating scheme 1. In this case the rating scheme is applied to the power source of the detection device.

Table 4-2: Sample rating scheme 1 example

Battery Operable	
Green 🟢	Common Battery used/long life
Yellow 🟡	Specialty Battery/long life Common Battery/short life
Red 🔴	Not battery operated/Specialty battery /short life

Sample rating scheme 2
The second rating scheme is similar to those commonly found in questionnaires. It has five rates ranging from extremely poor to excellent. The advantage of this scheme is that it familiar to most people. The disadvantage is that it is not as visual as the previous scheme.

Table 4-3: Sample rating scheme 2

Sample rating scheme 2	
Excellent	Highest capability
Good	Medium-high capability
Acceptable	Medium capability
Poor	Low-medium capability
Extremely poor	Lowest or no capability

Table 4-4 illustrates an example of the use of this rating scheme. It is an agreed upon rating scheme based on the percentage of common explosives that the device is able to detect.

Table 4-4: Sample rating scheme 2 example

Explosives Detection	
Excellent	90+% of explosives
Good	70 – 90% of explosives
Acceptable	50 – 70% of explosives
Poor	30 – 50% of explosives
Extremely poor	Less than 30% of explosives

Sample rating scheme 3
Example scheme 3 (see Table 4-5) is a blend of the first two schemes. It uses a familiar rating scheme while retaining a visual element that can make comparisons easier.

Table 4-5: Sample rating scheme 3

Sample rating scheme 3	
●	Highest capability
◕	Medium-High capability
◑	Low-Medium capability
◔	Lowest capability
○	No capability
⊗	Not specified

In this case, the ability of a chemical detector to detect chemicals in different states is evaluated in Table 4-6.

Table 4-6: Sample rating scheme 3 example

Detection States	
●	Detects chemicals in all three states
◕	Detects chemicals in two states
◑	Detects chemicals in one state
○	No capability
⊗	Not specified

(Source: Fatah 2007c)

Sample rating scheme 4

This is the most detailed of the rating schemes. It is a modification of scheme 2. It has the addition of five more rating possibilities making it a “shades of gray” scale. Certain characteristics of the detection device may require the rating scheme to be more precise. This scheme would afford that level of detail.

Table 4-7: Sample rating scheme 4

Sample rating scheme 4	
10 Excellent	Highest capability
9	
8 Good	Good capability
7	
6 Acceptable	Acceptable capability
5 Acceptable	Acceptable capability
4	
3 Poor	Poor capability
2	
1 Extremely poor	Lowest or no capability

Table 4-8 provides an example application of rating scheme 4. This is an extension of the example in Table 4-4.

Table 4-8: Sample rating scheme 4 example

Explosives Detection	
10 Excellent	90+ % of explosives
9	80 – 90% of explosives
8 Good	70 – 80% of explosives
7	60 – 70% of explosives
6 Acceptable	50 – 60% of explosives
5 Acceptable	40 – 50% of explosives
4	30 – 40% of explosives
3 Poor	20 – 30% of explosives
2	10 – 20% of explosives
1 Extremely poor	0 – 10% of explosives

At present, these rating schemes are presented only as a concept and have not been defined for each detection device characteristic. As we progress toward a standardized testing framework an appropriate rating scheme will need to be identified for each of the characteristics of the CBRNE detection device.

4.3 Rating levels

As each of the characteristics and their rating schemes are defined the rating levels will also need specification. As seen in the examples, the rating scheme can be specified in several ways.

- Qualitative measure such as: extremely poor to excellent
- % of active agents detected

- Probabilities such as probability of detection p_d.
- Time in seconds
- Weight in kilograms

4.4 *Maintenance of the rating scheme and rating levels*

Once the operational testing framework has been standardized, these rating schemes with their associated rating levels will need to be maintained and are expected to evolve as the CBRNE detection device sector evolves. It is reasonable to consider that an annual or biannual review of the rating scheme and the rating levels will be necessary to ensure relevance and accuracy.

5 Reporting guidelines

5.1 Introduction

The final step in operational testing is the creation of the operational testing report. This is a critical step in that this is where all of the work that has been completed up to this point is consolidated and presented in a well formatted and concise way. Care should be given to present the information in such a way as to satisfy the needs of the primary shareholder, the end-user community. Section 5.2 below presents one possible reporting format. This format is fairly standard in design within the field of testing in general. The only critical deviation from a standard format is the inclusion of the characteristics tables. The characteristics tables presented in section 5.3 are a first attempt at consolidating the information gathered during operational testing. Each of the fields in CBRNE detection has its own table. At present the tables are virtually identical. The tables' present standard reporting items such as: detector name, sensitivity, and specificity as well as items which are particular to operational testing such as: durability, safety, and ease of use. As the operational testing framework progresses it is likely that the table items will likely diverge regarding what items are presented.

The final issue is the standardization and acceptance of a given reporting format and the characteristics tables. What is presented here is simply a first attempt at a standard way of presenting the testing information. It would be extremely advantageous to all involved to have this issue resolved as early as possible in the development of the operational testing framework and of testing standardization.

It should be noted that the suggested characteristics tables are not intended to interfere with laboratory testing of technical parameters according to existing standards (e.g. for RN detectors). Results from such testing can be introduced as a summary in the operational testing scheme, as appropriate (e.g. to quantify "optimum" thresholds for detector sensitivity under field conditions).

5.2 Suggested reporting format

1. Introductory information

- Test centre that conducted the tests.
- Date and location of the tests.
- Individual(s) involved in the tests.
- Revision history

2. Device description

Present a description of the device that was tested to include:

- Manufacturer
- Intended use of device
- Technology used
- Other tests conducted or certifications that the device might have

3. **Test methodology used**
    - Test equipment used
    - Protocols used(e.g. standards, expert-defined protocols)
    - etc
4. **Tests conducted**
    - Scenarios
    - Combinations of active agents, interferents, and simulants

5. **Findings and results obtained in the testing**
    - Test log
    - Test documentation
    - Test data sheets
    - Analysis and conclusions

6. **Data field table**
    - Present data in the characteristics tables presented below

7. **Discussion and summary**
    - Present conclusions derived from the tests
    - Report any other relevant test information

8. **Recommended certificate**
    - Once a formal certification scheme has been created, present the certificate recommendations here

5.3 Characteristics tables

Table 5-1: Chemical characteristics table

Data Field	Rating Scheme		Notes
General			
Detector name			
Manufacturer			
Technology used			
Application			
Operational			
Chemical agents detected			
Confidence interval for sensitivity			
Confidence interval for specificity			
# of false positives			
# of false negatives			
Sample preparations			
Detection state			
Resistance to interferents			
Start-up time			
Response time			

Data Field	Rating Scheme		Notes
Time for data analysis			
Alarm type & effectiveness			
Environmental conditions			
Durability			
Ease of use			
Decontamination protocol			
Physical			
Size			
Weight			
Power requirements and capabilities			
Mobility/transportability			
Logistical			
Calibration required			
Repairs required			
Shelf life			
Unit cost			
Maintenance cost			
Consumables required			
Cost of consumables			
Special			
Operator skills required			
Training required/availability			
Manuals quality/availability			
Communications capability			
Security			
Warranty			
Applicable regulations			

Table 5-2: Biological characteristics table

Data Field	Rating Scheme		Notes
General			
Detector name			
Manufacturer			
Technology used			
Application			
Operational			
Biological agents detected			
Confidence interval for sensitivity			
Confidence interval for specificity			
# of false positives			
# of false negatives			
Sample preparations			
Detection state			

Data Field	Rating Scheme		Notes
Resistance to interferents			
Start-up time			
Response time			
Time for data analysis			
Alarm type & effectiveness			
Environmental conditions			
Durability			
Ease of use			
Decontamination protocol			
Physical			
Size			
Weight			
Power requirements and capabilities			
Mobility/transportability			
Logistical			
Calibration required			
Repairs required			
Shelf life			
Unit cost			
Maintenance cost			
Consumables required			
Cost of consumables			
Special			
Operator skills required			
Training required/availability			
Manuals quality/availability			
Communications capability			
Security			
Warranty			
Applicable regulations			

Table 5-3: Radiological/Nuclear characteristics table

Data Field	Rating Scheme		Notes
General			
Detector Name			
Manufacturer			
Technology used			
Application			
Operational			
Radionuclides detected			
Confidence interval for sensitivity			
Confidence interval for specificity			
# of false positives			

Data Field	Rating Scheme		Notes
# of false negatives			
Sample preparations			
Detection state			
Resistance to interferents			
Start-up time			
Response time			
Time for data analysis			
Alarm type & effectiveness			
Environmental conditions			
Durability			
Ease of use			
Decontamination protocol			
Physical			
Size			
Weight			
Power requirements and capabilities			
Mobility/transportability			
Logistical			
Calibration required			
Repairs required			
Shelf life			
Unit cost			
Maintenance cost			
Consumables required			
Cost of consumables			
Special			
Operator skills required			
Training required/availability			
Manuals quality/availability			
Communications capability			
Security			
Warranty			
Applicable regulations			

Table 5-4: Explosives characteristics table

Data Field	Rating Scheme		Notes
General			
Detector Name			
Manufacturer			
Technology used			
Application			
Operational			
Explosives detected			

Data Field	Rating Scheme		Notes
Confidence interval for sensitivity			
Confidence interval for specificity			
# of false positives			
# of false negatives			
Sample preparations			
Detection state			
Resistance to interferents			
Start-up time			
Response time			
Time for data analysis			
Alarm type & effectiveness			
Environmental conditions			
Durability			
Ease of use			
Decontamination protocol			
Physical			
Size			
Weight			
Power requirements and capabilities			
Mobility/transportability			
Logistical			
Calibration required			
Repairs required			
Shelf life			
Unit cost			
Maintenance cost			
Consumables required			
Cost of consumables			
Special			
Operator skills required			
Training required/availability			
Manuals quality/availability			
Communications capability			
Security			
Warranty			
Applicable regulations			

6 Other considerations

6.1 *Cost/benefit for operational testing and standardization*

There are numerous benefits that can be derived from the inclusion of operational testing and test standardization:

1. The results of operational testing will give the end-user a better understanding of the capabilities of the detection device in real world conditions.
2. The end-user will be able to determine if a device is applicable to their specific set of requirements.
3. Standardization will level the playing field. No test facility will be able to make the claim that their testing protocols are more stringent than any other.
4. Standardization will facilitate the mutual recognition of the testing. A manufacturer will be able to have their CBRNE detection device tested in one country and have this testing be recognized throughout the European Union.
5. In reference to item 4, this will not reduce the individual test cost but will reduce the cost of multiple tests.

6.1.1 Cost of testing

The biggest question surrounding the inclusion of operational testing is that of cost. According to our experts at Seibersdorf Labor, the laboratory testing of a spectroscopic portal monitoring system will cost approximately 100,000 Euros. The testing according to the standards comprises not only radiological tests, but also mechanical (shock, immersion of powder or water), electrical (electromagnetic compliance, electrical safety) and environmental (temperature variation, temperature shock) tests. Accordingly, radiological tests contribute only for 30-50 % of the total costs for device testing.

In addition to this single test cost there is a cost of testing in multiple countries. At present there is no reciprocity between countries. Having the testing done in one country does not imply that any other country will accept the results. This means that if a manufacturer wants to sell their product in Germany and England the manufacturer will be obliged to have the testing done in both countries. The addition of operational testing could potentially raise this single test cost. However, there are possible solutions to mitigate the cost of the additional testing.

6.1.2 Cost mitigation: a potential solution

There are several aspects to CBRNE threats: terrorist attacks, natural disasters, and industrial accidents. However, the main focus from the member states and the EU is on the first aspect, terrorism. As such the issue is not a local one. It is national and regional in nature.
Therefore it would seem logical that the effort surrounding the development of operational testing and conventional laboratory testing and the standardization of each should be driven from the very top within the European Union. The EU Commission should be given the

authority to delegate such development to organizations such as the European Defence Agency, who in turn would be responsible for making the standards law and for raising funding.

6.1.3 Funding

Testing of detection systems is expensive. Up to now, tests are performed by manufacturers during development of new systems and/or by end-users to collect data in the procurement process or after purchase – to find out capabilities of equipment under realistic conditions. In both cases there is no incentive to share testing results with other parties and costs have to be covered by the organization, who ordered the testing.

If testing of CBRNE detection systems should be done on a regular basis, there needs to be a political decision, regarding who is going to fund the associated technical efforts.
One practical example, how testing of detectors could be financed for the benefit of all stakeholders' incl. manufacturers and end-users, has recently been launched. The project will be funded on a full-cost basis by the European Commission, and is named:
I-Ispra: illicit trafficking radiation assessment programme (ITRAP+10) (JRC 2010).
The Commission will undertake the ITRAP+10 project through administrative arrangements (AA) with the Joint Research Centre (JRC). The purpose of this arrangement is to provide support to DG JLS (Justice, Freedom and Security) in the field of radiological/nuclear security. EU partner laboratories will be asked by a specific call to collaborate with the JRC on the assessment of the test procedures and equipment performances for some of the families of border monitoring instrumentation. Tests carried out during this project will focus on the nuclear/radiological performances of the border monitoring instruments (i.e. excluding the mechanical, electromagnetic, environmental tests, etc.). The tests will be mainly based on the technical specifications described in the corresponding European and/or international standards. Collaborating experts and laboratories get costs for personnel and consumables refunded by the project budget. Manufacturers are asked to offer equipment to be tested. This means, for the cost of one piece of equipment they get a full evaluation of the instrument for free. Project duration is approximately two years and it will start in early summer 2010.

6.2 Security of information and dissemination

Operational Testing Framework
At present, the operational testing framework is classified as PUBLIC and could be made available without restriction. There are two reasons for it being classified in such a way at this time. First, the information and concepts contained herein are not developed to a high degree. Virtually all of the information contained herein can easily be found on the internet or in a local library. Second, this is a first step towards an operational testing framework. The unlimited distribution at this time can facilitate further development of the document. A broad discussion within the stakeholder community is welcome.

Evolution
The operational testing framework document is a living document. As such, as time goes on, many of the concepts, methodologies, and information contained in this document will be

expanded and elaborated upon. The scenarios will become more formal and detailed. The information regarding the simulants, Interferents, and active agents and their use will become more detailed and complete. The testing concepts which are only introduced in this version of the document should be transformed into formal and specific testing procedures in the framework of future initiatives or funded projects.

End state

At some point in the future it will be warranted to classify the operational testing framework as EU RESTRICTED. This will be necessary for several reasons.

- Background information: the background information presented will go beyond what could reasonably be gotten from any open source. This level of detail could be useful for any organization planning to use CBRNE devices for their own reasons.
- Test procedure elaboration: the detailed presentation of the testing procedures could allow individuals that are interesting in using CBRNE devices to gain insight into the capabilities and limitations of the detection devices or infer possible short-comings of our testing procedures.
- Scenario elaboration: once the scenarios have been elaborated completely, it could give terrorists, non state actors, or rogue states a better idea about our focus in scenarios and testing and to gain knowledge in how to circumvent our detection devices.

Clearance and need to know

Once the operational testing framework is classified as EU RESTRICTED or above, it will require the individuals requesting the document to possess an appropriate security clearance to gain access to the document. In addition to the security clearance, the requestor should be able to present his/her need to know. Essentially, the requestor will have to make clear WHY they should be given access to the document.

The testing report

The output of the operational testing framework document will be a device evaluation report. The final format and details of this report are still under development but some suggestions have been made in Sections 5 and 6 of this document. What is clear is that this report is designed for the end-user community as a means to do a comparison of the available CBRNE detection devices. It will make it possible for the end-users to find a detection device that is appropriate for their application and that is based on a mixture of qualitative and quantitative measures and is systematic in its testing approach.

With respect to the distribution level of the report: it is recommended that it be classified at the same level as the operational testing framework. Of course, whoever will be responsible for the funding of operational testing, will make the decision on the potential dissemination of testing results. From our point of view, it is desirable to make results available to end-users in order to share existing knowledge and make the best out of limited resources available for CBRNE detector testing.

7 Conclusion and recommendations

The operational testing framework (OTF) lays the groundwork for further development of an operational testing protocol for CBRNE detection systems. The document is designed to illuminate many of the issues surrounding operational testing. The major goal of this deliverable has been defined to draw attention and initiate a focussed discussion within the CBRNE stakeholder community on the usefulness of the suggested approach and – if accepted - to further develop such a concept. On purpose a wide variety of related topics is addressed and sometimes optional information given; any prioritization of topics has been avoided not to deviate the discussion into any specific direction, but leave the final decision on the most suitable concept and necessary testing components with the stakeholders.
Contained within the text there is an introduction to the CBRNE field: each detection focus (C, B, RN, and E), their associated threats and technologies used. Following that we present the rationale for the inclusion of operational testing. Namely, that laboratory testing alone doesn't provide a complete picture of the capabilities of a detection system. Then cornerstone of operational testing, the scenario is introduced. Human factors are discussed briefly with an example to illustrate the process of test development. In the later chapters, issues such as the tests to be considered, possible rating schemes, and ideas for the reporting format of an operational test are suggested. We finish with a discussion of the cost/benefit of operational testing and the distribution of the OTF and the results from testing. All that is presented is to allow the reader to gain a general understanding of the issues surrounding the testing of CBRNE detection systems without going into too much detail.

Recommendations

This version of the operational testing framework is only an introduction. Some improvement is expected to be gained from the Creatif Deliverable 3.2 (End-user feedback questionnaire) and can be incorporated in the final version of the OTF deliverable, although up to now the response is limited.

Nevertheless, it is recommended that further projects be created to investigate and elaborate in more detail the issues brought up in this document. In particular, a real proof of concept in terms of testing exercises with end-user involvement seems to be a very interesting idea.

The threat from CBRNE incidents is not confined within national borders nor is it purely an issue of one countries' national security. An incident in one member state will likely have grave affects in numerous other member states. With shared power networks, road and rail networks and with the free movement of people and goods the issue becomes one that is a possible threat to the European Union as a whole. The collective use of CBRNE detection systems is done not only to protect locally but EU wide. The testing of such CBRNE detection systems should also be treated in a similar fashion. Therefore, a European approach to the development of operational testing seems necessary. Although there may be differences in the national doctrines of end-user organizations and operational habits, it is even more important to take into account cross-country and cross-organizational cooperation. To our understanding, scenario-based testing could be a suitable mean to find out common understanding on the most efficient use of CBRNE detection systems without unwanted generalizations. This could help to diminish rather than pronounce operational differences in the use of detectors throughout Europe or different end-user organizations.

Specific issues to be covered by dedicated project initiatives could be:

- **Operational scenario development:** Development of the scenarios so that there is sufficient detail to make them useful as a script in the testing and cover specific operational needs of different user-groups (e.g. fire brigade; customs officers)
- **Operational test development:** Based on the scenario scripts: develop specific testing procedures that address the testing requirements alluded to in section 3.4 of this document
- **Standardization:** To be effective, the operational testing framework needs to be standardized on a European level.
    - Rating schemes and levels
    - Reporting: to include format and reportable items
    - Test facilities (in part addressed in work package 4 of CREATIF)

8 References

Adams, C., (2010) Human Factors [online] Available at: http://ergonomics.about.com/od/glossary/g/defhumanfactors.htm [Accessed 10 May 2010].

American National Standards Institute, 2008. N42.48-2008: American National Standard. Performance Requirements for Spectroscopic Personal Radiation Detectors (SPRDs) for Homeland Security. New York: IEEE Inc.

American National Standards Institute, 2006. N42.34-2006: American National Standard. Performance Criteria for Hand-Held Instruments for the Detection and Identification of Radionuclides. New York: IEEE Inc.

Christesen, S. Gonser, K. Lochner, J.M. Sedlacek, A. Chyba, T. Sink, D. Jones, J.P. Corrado, B. & Slaterbeck, A., 2004. UV Raman Detection of Chemical Agents UV Raman Detection of Chemical Agents UV Raman Detection of Chemical Agents. Orlando: Proceedings of Army Science Conference (ASC).

Christesen, S.D. Lochner, J.M. Hyre, A.M. Emge, D.K. & Jones, J.P., 2006. UV Raman spectra and cross sections of chemical agents. In: P. J. Gardner, A. W. Fountain III (Eds.), Chemical and Biological Sensing VII, Vol. 6218, pp. 8.

Clark, J.M. Kaye, P.H. Hirst, H. & Reid, K., 1993. Complementary techniques for the analysis of the shape of airborne particles. J Aerosol Sci. 24, S243-S244.

Committee on Commercial Aviation Security Panel on Assessment of Technologies Deployed to Improve Aviation Security, 1999. Assessment of Technologies Deployed to Improve Aviation Security, First Report. Washington DC: National Academy Press.

Council of the European Union, 1996. Council Directive 96/29/EURATOM: Basic safety standards for the protection of the health of workers and the general public against the dangers arising from ionic radiation. Brussels: Official Journal of the European Community

Eiceman, G. Boyett, C. & Parmeter, J., 1999. NIJ Report 100-99: Evaluation of a Test Protocol for Explosives Trace Detectors Using a Representative Commercial Analyzer. Gaithersburg, MD: Office of Law Enforcement Standards, National Institute of Standards and Technology.

Ellis-Steinborner, S.; Johnson R., 2007. DSTO-TR-2033: Standard Protocol for Evaluation of Explosive Detection Equipment. Edinburgh South Australia: Weapons Systems Division Defence Science and Technology Organization.

Engelbrecht, R. Schwaiger, M. & Ågren, G., 2006: Nuclear and Radiological Detection Equipment - Technology Review and Requirements. IMPACT WP300, deliverable D300.2a, 121 pp.

European Economic Community, 1989. Council Directive 89/686/EEC: On the approximation of the laws of the Member States relating to personal protective equipment. Brussels: Official Journal of the European Community.

Fatah A. et al., 2007. Guide 101-6: Guide for the Selection of Biological Agent Detection

Equipment for Emergency First Responders, 2nd ed. Gaithersburg, MD: Office of Law Enforcement Standards, National Institute of Standards and Technology

Fatah A. et al., 2007. Guide 100-6: Guide for the Selection of Chemical Detection Equipment for Emergency First Responders, 3rd ed. Gaithersburg, MD: Office of Law Enforcement Standards, National Institute of Standards and Technology

Fatah A. et al., 2007. Guide 102-6: Guide for the Selection of Personal Protective Equipment for Emergency First Responders, 2nd ed. Gaithersburg, MD: Office of Law Enforcement Standards, National Institute of Standards and Technology

Fitch, J. Raber, E. & Imbro, D. 2003. Technology challenges in responding to biological or chemical attacks in the civilian sector. SCIENCE. 302, 1350-1354.

Hairston, P.P., Ho, J., Quant, F.R., 1997. Design of an instrument for real-time detection of bioaerosols using simultaneous measurement of particle aerodynamic, size and intrinsic fluorescence. J Aerosol Sci. 28, 471-482.

Ho, J., 1996. Real time detection of biological aerosols with fluorescence aerodynamic particle sizer (FLAPS). J Aerosol Sci. 27, 5581-5582.

Ho, J., Spence, M., 1998. Background Aerosol Characteristics Measured with a Fluorescence Aerodynamic Particle Sizer: Sensitivity of FLAPS Performance. S:. SM 1504, 3-43.

Joint Research Center (2010) I-Ispra: Illicit Trafficking Radiation Assessment Program (ITRAP+10 Project) [online] Available at: http://web.ec.jrc.europa.eu/callsfortender/index.cfm?action=app.showdoc&id=5622

Kaye, P.H. Barton, J.E. Hirst, E. Clark, J.M., 2000. Simultaneous light scattering and intrinsic fluorescence measurement for the classification of airborne particles. Appl Opt. 39, 3738-3745.

Kaye, P.H. Eyles, N.A. Ludlow, I.K. & Clark, J.M., 1991. An instrument for the classification of airborne particles on the basis of size, shape, and count frequency. Atmos Environ. 25A, 645-654.

Lake, B. Schulze P., 2008. Guidelines for Mass Casualty Decontamination During a HAZMAT/Weapon of Mass Destruction Incident. Volume II. Aberdeen Proving Grounds: U.S. Army Edgewood Chemical Biological Center.

Lancelin, H. Bleuse, P. & Clausin, P., 2004. Method and device for the detection of the presence, and real-time analysis of, chemical and/or biological substances in the athmosphere, Patent cooperation treaty application.

Lancelin, H. Guene, G. Bleuse, P. & Clausin, P. 1999. Apparatus combining spectrophotometry and flame ionization detection for analysing a gas composition, Patent cooperation treaty application.

Marshall, M. Oxley, J., 2009. Aspects of Explosives Detection. 1st ed. Amsterdam NL, Elsevier.

O'brien, T. Charlton S., 2002. Handbook of Human Factors Testing and Evaluation. 2nd ed. New Jersey: Mahwah.

Rapport, I. Balkcom, G. Stirrat, C. & Wilson , R., 1996. System-Level Testing in Operational Environments. Johns Hopkins APL Technical Digest, Volume 17, Number 4.

Rittfeldt, L. Fällman, Å., 2005. Detection of chemical warfare agents in water by solid phase microextraction-ion mobility spectrometry (SPME-IMS). FOI-R--1687--SE.

Theisen, L., 2005. Survey of Commercially Available Explosives Detection Technologies and Equipment 2004. Rockville MD: National Criminal Justice Reference Service.

USACHPPM, 2008: Health-Based Chemical Vapour Concentration Levels for Future Systems Acquisition and Development. USACHPPM Tech. Report No. 64-FF-07Z2-07, US Army Center for Health Promotion and Preventative Medicine, Aberdeen Proving Ground, MD, 21010, 95 pp.

ANNEX A: Relevant definitions

Included in this document is a dictionary. This is as excerpt of the CREATIF deliverable D.1.1 “Glossary to define common language and delimitations for testing evaluation and certification”. The glossary is designed to be a resource for anyone involved in the testing of CBRNE detection devices. At present, the dictionary is not all inclusive but will evolve and developed as the operational testing framework becomes more mature.

Term	**Definition**
Acceptance test	A contractual test to prove to the customer that the device meets certain conditions of its specification.
Accredited testing laboratory	Testing laboratory that has been accredited by an authoritative body with respect to its qualification to perform verification tests on the type of instruments covered by applicable standards or specific protocols.
Aerosol	A suspension of finely divided liquid or solid particles suspended in a gaseous form. They are solid or liquid substances classified as dusts, fumes, smokes, mists, and fogs according to their physical nature, particle size, and method of generation. Particle size may vary from 100 micrometers (µm) to 0.01 in diameter.
Alarm (Detector)	An audible, visual, or other physical signal activated when the instrument reading exceeds a preset value or falls outside of a preset range.
Alert / Alarm	Any kind of physical fact that lunches the intervention of FRs.
APR	Acronym for: Air Purifying Respirator.
B-detection	Aim is to determine the presence of any biological danger for people living and breathing in a given place. Bio-detectors can ely on physical measurements or on biological assays.
B-incident	An incident where pathogenic micro organisms constitute a danger regardless if the origin is: - An accident emitting pathogenic substances - A natural dispersion of pathogenic substances - A deliberate dissemination through terrorism or other criminal activity - An attack with biological weapons
Biological Agents	A micro-organism or product of a micro-organism intended to cause disease in man, plants, or animals or causes the deterioration of material.
Bulk detection	Detection technologies able to detect explosive particles in bulk (mode).
CBRNE alarm	An indication from any source that a chemical, biological, radiological or nuclear or Toxic Industrial Hazard is present.

Term	Definition
	Related term Alert, Emergency Alarm.
CBRN defence	Plans and activities intended to mitigate or neutralize adverse effects on operations and personnel resulting from: the use or threatened use of Chemical, Biological or Nuclear weapons and devices; the emergence of secondary hazards arising from counter-force targeting; or the release, or risk of release, of Toxic Industrial Materials into the environment.
CBRN devices	An improvised assembly or process intended to cause the release of a chemical or biological agent or substance or radiological material into the environment or to result in a nuclear explosion.
CBRN environment	Conditions found in an area resulting from immediate or persisting effects of CBRN hazards also resulting from the release of Toxic Industrial Materials (TIM). The term CBRN environment as used in this document refers to an environment in which: a. At least on of the adversaries possesses the capability to use CBRN weapons and/or devices and has threatened to employ them; b. The risk or threat of the deliberate or accidental release of TIM has been assessed and/or identified; c. CBRN weapons and/or devices have been used and the possibility exists that these weapons and/or devices could be employed again; d. The effect from CBRN or TIM hazards persist in the area of operation to a level requiring forces to take CBRN defence measures.
CBRN hazards	CBRN hazards result from the employment by any means of CBRN weapons or devices or the release of Toxic Industrial Materials resulting in the contamination or irradiation of personnel or the environment, are or any particular object. CBRN hazard result from: a. The employment of chemical agents b. The employment of biological agents c. The employment of nuclear weapons or radiological devices resulting in nuclear radiation caused by fallout, artificial dispersion of radioactive material, or irradiation and d. The release of toxic industrial materials. For the purpose of this document the word substance is used as an overarching generic term.
CBRN incident	Any occurrence involving the emergence of chemical, biological, radiological or nuclear and toxic industrial hazards or effects,

Term	Definition
	irrespective of source, cause or intent
CBRN materials	Weaponized or non-weaponized chemical, biological, radiological or nuclear materials that can cause significant harm to human beings.
CBRN weapons	A fully engineered assembly designed for employment by the armed forces of a nation state to cause the release of a chemical or biological agent or radiological material onto a chosen target or to generate a nuclear explosion.
CBRN	Acronym for: Chemical, Biological, Radiological and Nuclear
Certification	The process of officially recognizing that organizations, individuals, material or systems meet defined standards or criteria. Note: In the context of military forces, the hierarchical relationship in logical sequence is: assessment, analysis, evaluation, validation and certification.
Chemical Agents	A chemical substance which is intended for to kill, seriously injure, or incapacitate man through its physiological effects. The term excludes riot control agents when used for law enforcement purposes, herbicides, smoke and flames.
C-incident	An incident where the effects of toxic chemicals are a hazard, regardless of the origin: - An accident during transport, storage or production of chemicals. - Deliberate dissemination through terrorism or other criminal activities. - An attack with CWA.
CWA	Acronym for: Chemical Warfare agent.
Decontamination	The process of making any person, object, or area safe by absorbing, destroying, neutralising, making harmless, or removing chemical, biological or radioactive agents.
Detection	Detection aims at establishing the release or discovering the presence of a CBRNE agent in a given area/location. Detection is usually associated with prevention. In reality, detection mechanisms are needed at the three stages of a CBRNE incident, i.e. before, during and after an event.
Detection limits	The extremes of detection or quantification for the CBRNE material of interest.
Detector	A device employed to discover the emergence, presence or absence of chemical, biological, radiological and nuclear hazards. Detector types are: a. Point detector. A detector that reacts automatically to

Term	Definition
	hazards at the point of interception. b. Stand-off detector. A detector that reacts to distant incidents or hazards. c. Remote detector. A point or stand-off detector employed at a distance from protected force element.
Dissemination	Basic parameter of a CBRN scenario description. Includes • ***Amount*** of agent distributed (measured by weight) • ***Vector*** – Means and medium for dispersion (air, ventilation system, water distribution, contaminated ground material or equipment or material such as door handles, banisters, instruments etc). • ***Equipment*** used for dissemination (Green house sprayer, explosive device, crushed bottle etc.) • ***(Immediate progress) Fate*** – Describes secondary vector or contamination in the immediate phase (e.g. spill that evapourates, infected people moving and spreading disease etc.) • ***Particle size distribution*** – percentage of the dispersed agent that is expected to be respirable particles
Effects	Basic parameter of a CBRN scenario. Effects may be divided into first, second and third order of effect. • A ***first order effect*** is the immediate consequence of a terrorist attack, which could inflict disease or physical damage on humans, animals and plants. The first stage also includes FRs such as police, health care, and fire brigades. • The ***second order effects*** are the immediate impact on societal function which are the consequences of first order effects spreading to sectors other than those immediately involved. • The ***third order effects*** include all sectors of society and have impact on economic viability and political stability.
E-incident	An incident where the effects of explosive chemicals are a hazard, regardless of the origin. • An accident during transport, storage or production of chemicals. • Deliberate dissemination through terrorism or other criminal activity. An attack with explosives.
Explosive substance	A chemical substance (or mixture of materials) intended to produce an explosive effect in civil applications (explosives for mines and quarries avalanche release,…), military or terrorist applications.

Term	Definition
False alarm	Alarm NOT caused by a threat under the specified background conditions.
False-negative	Failing to detect a real threat.
False-positive	Detecting a non-existent threat.
First responder	The first trained persons to attend or arrive at an incident. Persons include the fire brigade, police and ambulance services. A FR’s role lasts (more or less) up to 4 hours (and in most cases less than 24 hours).
Fixed detectors	Fixed detectors are installed, automatic instruments designed to be used at checkpoints of critical facilities to monitor a continuous flow of persons, vehicles, and luggage, cargo or air samples.
Hand-held device	Hand-held devices are lightweight instruments, which can be used to detect, locate and sometimes identify a CBRNE agent.
Hazardous materials	Any material that is flammable, corrosive, an oxidizing agent, explosive, toxic, poisonous, etiological, radioactive, nuclear, unduly magnetic, a chemical agent, biological research material, compressed gases, or any other material that, because of its quantity, properties, or packaging, may endanger human life or property.
Improvised explosive device	A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic or incendiary chemicals and designed to destroy, incapacitate, harass or distract. It may incorporate military stores, but is normally devised from non-military components.
Incident	See: • C-incident • B-incident • R- and N-incidents
Monitoring (Detector)	Monitoring is defined as the continuous or periodic process of determining the presence or absence of chemical, biological or radioactive or toxic industrial hazards. This may or may not include quantification.
Personal protective equipment	The personal clothing and equipment required to protect an individual from biological and chemical hazards and some nuclear effects. This ordinarily includes but must not be limited to a respirator, whole body covering and simple detection, decontamination and first-aid devices.
Plastic explosive	An explosive which is malleable at normal temperatures.
Point detection	Point detection refers to devices which can be pointed at a suspect area or be a point source for detection.

Term	Definition
Precision	Degree of agreement of repeated measurements of the same parameter.
Radioactive material	Radioactive material includes both special nuclear and radioactive material, unless otherwise specifically noted.
Reading	The indicated or displayed value of the readout.
Reliability	The detector gives the same result every time for a certain agent.
RN-detection	Structure of radiological detection equipment: • Health and Safety instruments: are used to give an alarm in the case of any harmful intensities of ionization radiation in surroundings and to monitor the received dose. • Hazard assessment instruments: are mainly meant to search for hot spots and radiation sources or to survey an area, and in some cases also give information of the radiation energy, and hence give the possibility to identify the radionuclide. • Mobile laboratories or portable instruments: are used for surveying larger areas or for radionuclide identification. • Measuring systems: include whole body counters, portal monitors, air filtering systems and stationary systems for monitoring environmental radiation levels, are used to prevent a further spread of the activity, or in the case of a spread, to assess the consequences.
Robustness	The detector functions appropriately independent on external conditions.
Screening	A systematic examination or assessment of a scene of intervention or a sample, done specifically to detect or to classify an unwanted substance or attribute.
Sensitivity	Lowest concentration to be detected within a prescribed test situation.
Standardization / normalization	The development and implementation of concepts, doctrines, procedures and designs in order to achieve and maintain the compatibility, interchangeability or commonality which are necessary to attain the required level of interoperability, or to optimize the use of resources, in the fields of operations, materiel and administration.
Standoff detection	Standoff detectors are stationary systems or mobile units designed to monitor large areas remotely.
Terrorist CBRN incident	Any kind of event that produces victims due to C,B,R, and N agents intentionally released by persons or dedicate devices to aggress the population could they be of military, industrial, natural or improvised origin.

Term	**Definition**
Test	A procedure whereby the instrument, circuit, or component is evaluated.
Toxic industrial chemical (TIC)	Any chemical toxic substance, whatever its physical phase, known for its toxicity, which can be variable in time or not.
Toxic industrial materials (TIM)	Toxic Industrial Materials (TIM) is a generic term fir toxic or radioactive compounds in solid, liquid, aerosolized or gaseous form. These may be used, or stored for use for industrial, commercial, medical, military or domestic purposes. TIM maybe chemical, biological or radioactive and described as Toxic Industrial Chemical, Toxic Industrial Biological, including pathogenic material (TIB) or Toxic Industrial Radiological (TIR).
Trace detection	Detection technologies able to detect CBRNE agents (often explosives molecules) in trace mode (very fine solid particles).
Validation	The confirmation of the capabilities and performance of organizations, individuals, material or systems to meet defined standards or criteria, through the provision of objective evidence.
Vapour detection	Detection technologies able to detect explosive molecules in vapour mode.

ANNEX B: Available standards

Table B-1: List of available standards regarding explosives detection equipment

ASTM E2520-07 2007	Standard Practice for Verifying Minimum Acceptable Performance of Trace Explosive Detectors
ASTM F2069 2000	Standard Practice for Evaluation of Explosives Vapour Detectors
DSTO-TR-2033 2007	Standard Protocol for the Evaluation of Explosives Detection Equipment
NIJ Report 100-99 1999	Evaluation of a Test Protocol for Explosives Trace Detectors Using a Representative Commercial Analyzer

Table B-2: List of IEC standards regarding RN detection equipment

IEC 62244 2006	Radiation protection instrumentation - Installed radiation monitors for the detection of radioactive and special nuclear materials at national borders
IEC 62327 2006	Radiation protection instrumentation - Hand-held instruments for the detection and identification of radionuclides and for the indication of ambient dose equivalent rate from photon radiation
IEC 62401 2007	Radiation protection instrumentation - Alarming personal radiation devices (PRD) for detection of illicit trafficking of radioactive material
IEC 62533 draft	Highly sensitive hand-held instruments for photon detection of radioactive material
IEC 62534 draft	Highly sensitive hand-held instruments for neutron detection of radioactive material
IEC 62484 draft	Spectroscopy-Based Portal Monitors used for the Detection and Identification of Illicit Trafficking of Radioactive Material
IEC 62618 draft	Radiation protection instrumentation – Spectroscopy-based alarming personal radiation devices (SPRD) for detection of illicit trafficking of radioactive material

Table B-3: List of available ANSI standards regarding RN detection equipment

N42.32 2006	American National Standard Performance Criteria for Alarming Personal Radiation Detectors for Homeland Security
N42.33 2006	American National Standard for Portable Radiation Detection Instrumentation for Homeland Security
N42.34 2006	American National Standard Performance Criteria for Handheld Instruments for the Detection and Identification for Radionuclides

N42.35 2006	American National Standard for Evaluation and Performance of Radiation Detection Portal Monitors
N42.37 2006	American National Standard for Training Requirements for Homeland Security Purposes Using Radiation Detection Instrumentation for Interdiction and Prevention
N42.38 2006	American National Standard Performance Criteria for Spectroscopy Based Portal Monitors Used for Homeland Security
N42.39 draft	American National Standard for Performance Criteria for Neutron Detectors for Homeland Security
N42.41 2007	American National Standard Minimum Performance Criteria for Active Interrogation Systems Used for Homeland Security
N42.42 2006	American National Standard Data Format Standard for Radiation Detectors Used for Homeland Security
N42.43 2007	American National Standard for Performance Criteria for Mobile and Transportable Radiation Monitors Used for Homeland Security
N42.44 draft	Performance and evaluation of checkpoint cabinet x-ray imaging security-screening systems
N42.45 draft	Evaluating the image quality of x-ray computed tomography security-screening systems
N42.46 draft	Measuring the performance of imagining x-ray and gamma-ray systems for cargo and vehicle security screening
N42.47 draft	Measuring the Imaging performance of X-ray and Gamma-ray Systems for Security Screening of Humans
N42.48 2007	American National Standard for Performance Requirements for Spectroscopic Personal Radiation Detectors (SPRDs) for Homeland Security
N42.49A/B draft	Performance Criteria for Personal Emergency Radiation Detectors (PERDs) for Exposure Control

Table B-4: List of documents containing relevant IAEA standards

Nuclear Security Series 1, IAEA, 2006	Technical and functional specification for border monitoring equipment: reference manual
IAEA-TECDOC-1312, 2002	Detection of radioactive material at borders
the IAEA Coordinated Research Project	Improvement of Technical Measures to Detect and Respond to Illicit Trafficking of Nuclear Material and other Radioactive Material