HOTHREAT
CBRN

CBRNe VIP protection programme

Co-funded by
the European Union

hothreat.eu

Tailored CBRNe protection measures for hotels and conference centres

CBRNe VIP protection programme

Agreement no.: 101100555 — HOTHREAT

Funded by the European Union

Document introduction

WP number and title	WP3: Comprehensive CBRNe protection system
Deliverable full title:	D3.2 CBRNe VIP protection programme
Lead beneficiary/ Author	Polícia de Segurança Pública (PSP)
Contributor(s)	All consortium partners
Document type	Report
Last Update	18.09.2024
Dissemination level	Public

Acknowledgement:
This project is funded by the European Union's Internal Security Fund — Police. Grant Agreement No. 101100555 — HOTHREAT

This project is co-funded by the Polish Minister of Science and Higher Education in frames of the program "International Co-financed Projects"

Disclaimer:
The content of this document represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Project consortium

Research, expertise, technology providers

End-users

Law enforcement agencies

The material for this publication was developed and reviewed by the HOTHREAT consortium:

Partner organization name	Country
University of Lodz	PL
Dynamic Safety Corporation	PL
Polaris Hospitality Enterprises	PL
Hotel Boss	PL
Safety Core	PL
International Security and Emergency Management Institute	SK
National Institute of Aerospace Technology	ES
Atiram Hotels	ES
The Center for Security Studies	EL
Hellenic Police	EL
Konngruent	RO
Sigoria Security Solutions	PL
Center for Social Innovation	CY
Aphrodite Hills Resort	CY
The Nicosia Tourist Board	CY
Lodz Regional Police Headquarters	PL
Fondazione Safe	IT
Ministry of Internal Administration	PT
Department of Interior of the Government of Catalonia	ES

Table of content

Table of figures

List of tables

1. Introduction to the HOTHREAT project

Hotels, leisure and conference facilities have long been targets of terrorist attacks and the threat level is still increasing. Due to its characteristics this sector is vulnerable to attacks, and in last 25 years over 160 attacks were conducted. Chemical, biological and radiological/nuclear (CBRN) threats are emerging risks that the European public must take into consideration. Notably, the use of those agents can be often combined with explosive devices – CBRNe.

The HOTHREAT project aims to address the existing gap in the protection of hotels from CBRNe terrorist threats by bringing together a consortium composed of private and public entities, experts, end-users, security companies and law enforcement agencies. Indeed, the Consortium is composed of 19 partners from 8 EU Member States.

The main objective of HOTHREAT is to increase the safety of EU MS society from CBRNe threats by targeting hotels and conference centres (HCC). To do so, during the project cycle, comprehensive vulnerability and needs analysis will be conducted as well as best practices identification to elaborate tailor-made measures for CBRNe protection. The measures include recommendations for prevention, protection and response procedures. Moreover, CBRNe measures include recommendations for the adoption of protective equipment, multi-service communication models, programmes for VIP visits, cleaning services, food defence, epidemiology inquiries and CBRNe emergency application for mobile devices integrated with AR. Finally, training sessions will be delivered for hotel employees through a series of piloting and large-scale exercises to ensure the adoption of high-quality and well-addressed measures.

Specifically, Work package 3 is the core of the HOTHREAT project with the overreaching aim of creating a comprehensive system supporting HCC against CBRNe. This system is composed of 5 guidelines addressing CBNRe risks as follows: Recommendations for prevention, protection and response procedures to CBRNe terrorist act; Food protection guidelines; Guidelines for epidemiological enquiry; CBRNe VIP protection Programme; Cleaning services recognition & reaction Programme.

The document at hand represents a key project legacy thus contributing to the creation of a comprehensive system supporting HCC against CBRNe by providing a guideline on CBRNe VIP protection Programme.

2. Scope and objective of the guidelines

In an increasingly complex and interconnected world, the hospitality industry faces evolving challenges in ensuring the safety and security of its guests, particularly those of elevated status and prominence.

The 26/11/2008 terrorist attack on the Taj Hotel in Mumbai, India, had a profound and far-reaching impact on hotel security worldwide, leading to significant changes in security protocols, practices, and awareness within the hospitality industry.

Figure 1 The Taj Hotel Mumbai, in India

Source: Express photo by Ganesh Shirsekar

Some of those impacts were:

- The heightened security measures (surveillance, access control, and stricter screening procedures for guests, staff, and deliveries).
- Focus on crisis response and training (emergency procedures, evacuation protocols, first aid, and coordination with law enforcement and emergency services).
- Integration of technology to driven security solutions (CCTV cameras, access control systems, biometric scanners, and emergency communication systems).

- Collaboration with authorities (sharing intelligence, conducting joint training exercises, and developing coordinated response plans to address security threats effectively).
- Focus on guest communication and reassurance (implementing crisis communication protocols, establishing emergency hotlines, and utilizing digital platforms for real-time information dissemination).
- Enhanced risk assessment and management (threat landscape, analysing potential targets, and implementing countermeasures to deter attacks).

Overall, the terrorist attack on the Taj Hotel Mumbai served as a wake-up call for the hospitality industry, prompting a paradigm shift in how hotels approach security. It led to a more proactive, collaborative, and technology-driven approach to security management, aimed at ensuring the safety and well-being of guests, staff, and the broader community.

Furthermore, with the emergence of CBRNe threats as potential sources of harm and disruption, the need for proactive and robust security measures has become paramount.

The creation of a dedicated CBRNe protection program represents a critical step in addressing these challenges and safeguarding the well-being of the community visiting HCC, particularly individuals, dignitaries and high-level executives or VIP during their stays in hotels and participation in conferences and events.

These guidelines aim to provide a comprehensive framework to mitigate the risks posed by CBRNe threats, encompassing prevention, detection and response strategies tailored to the unique needs and vulnerabilities of customers in general and VIP in particular.

The significance of protecting VIP against CBRNe threats cannot be overstated. Beyond the immediate safety and security concerns, the presence of VIP in HCC often carries broader implications for public safety, political and economic stability, and national security.

Disruption or harm to VIPs can have far-reaching consequences, including reputational damage to hospitality establishments, loss of business revenue, and erosion of consumer confidence in the safety of travel and tourism destinations.

Moreover, the evolving nature of CBRNe threats, characterized by their clandestine and indiscriminate nature, underscores the importance of proactive risk mitigation measures and continuous preparedness efforts. As such, the development of a CBRNe VIP protection program represents a proactive and forward-thinking approach to security, aimed at staying ahead of emerging threats and ensuring the resilience and sustainability of the hospitality industry in the face of adversity.

This document seeks to provide guidance and recommendations for the creation and implementation of a robust CBRNe VIP protection program in HCC.

By examining the key components, strategies, and best practices associated with such a program, it aims to equip stakeholders with the knowledge and tools necessary to enhance the safety and security of VIPs and guests in an increasingly complex and dynamic threat environment.

The purpose of this task 3.4, integrated into WP3, is to collect and analyse good practices concerning HCC facilities' CBRN preparedness, security, response, and recovery to create and embed a CBRNe VIP protection programme into them,

The scope is include specific recommendations on CBRN security in the hospitality industry and produce recommendations for local security planning and cooperation with services associated with VIP visits, focusing on existing procedures when compared with CBRN requirements, eliminating contradictory solutions and suggesting areas where specific solutions are needed taking into account the specific entity, event, location and facilities.

3. Outcomes from WP2

Part of this document is the result of Work Package 2 (WP2) - Analysis of end users' needs, good practices, and relevant EU-funded projects, through deliverable 2.5 - the report summarizing the research findings on EU initiatives, that summarizes the input collected in this Work Package of the HOTHREAT project.

WP2 aimed to discover best practices, gaps, needs, and recommendations from public spaces and related infrastructure that can be transferrable to the context of HCC from research projects funded by the EU Commission, through Desk Research, Surveys, and Hotel Inspections.

Through the analysis of all the results obtained in the analysis of the relevant EU-funded projects, 132 items relevant and useful for the HOTHREAT research topics were obtained, of which only 2 are related to the issue of VIP Protection, 1 to the gaps, and another to the recommendations.

Desk Research - Summary of Best/Good Practices

TASK 2.2 DESK RESEARCH	Best/Good Practices	References
Other	General Practices / Solutions 1) Programs for VIP visits, cleaning services, food defence, epidemiology inquiries Specific Practices / Solutions 2) Outcomes from projects MALL CBRN, BULLSEYE, SAFE STADIUM	2: to be provided by partners

Table 1 Overview of the VIP topics concerning to best/good practices collected in desk research

Survey Research – Summary of Gaps, Needs and Recommendations

TASK 2.3 SURVEY RESEARCH	Gaps	Needs	Recommendations
VIP Protection	• Protection of VIPs in the own venue is considered low (10/13) to medium (3/13). Protection of VIPs vs CBRN attack is very low.	No needs from end-users partnersin this field as they not targeted on VIPs visits.	• Preparation of recommendations of rules of enhancing CBRN safety in the VIP targeted hotels (separated ventilation, protection of inlets, use of Colpro systems, etc.)

Table 2 Overview of the VIP topics concerning to gaps, needs and recommendations collected in survey research.

Hotel Inspections - Summary of Best/Good Practices and Recommendations

TASK 2.4 HOTEL INSPECTIONS	Best/Good Practices	Gaps	Recommendations
Hotel Cooperation with LEAs/Public Services	• Collaboration with the Police and the law enforcement agencies • Close cooperation with security services/agencies before VIP or high-risk events • Signed agreement with bus transportation company in case of a need to transfer evacuated individuals		• Conducting joint exercises with public services to enhance cooperation and practice security procedures

Table 3 Overview of the VIP topics concerning to best/good practices and recommendations collected in hotel inspections.

Methodology

A methodology for this task was developed based on the following principles:

- Identify all relevant topics necessary to be analysed and reported in WP3.
- Identify all relevant topics necessary to be addressed, developed and reported by other WPs.
- Cooperation and consistency in approach to all other WP analysis and reporting.
- Maximizing opportunities to gather as much relevant material as possible during each WP3 activity.
- Existing practices and procedures by Law Enforcement Agencies (LEA), mostly those who have responsibilities in the VIP protection.
- Known general principles observed by VIP security
- Practices and procedures implemented in HCC to prevent, detect and react to risks associated with the VIP and large events protection against CBRNe threats.

Information presented in this report are intended to be used during trainings and also for preparation of instructions, manuals, procedures or other documents relevant for increasing awareness and preparedness against CBRNe threats events in HCC.

Content of the guidelines

It is impossible to provide security for every eventuality and is not possible totally avoid the threat from CBRN agents. The goal of the project is to reduce risks of it and provides generic advice to prevent, detect and react to this risk, to minimize possible effect of this type of attack providing important information to all identified target groups relevant to CBRN security in HCC.

That information should then be adopted and implemented to interested HCC to:

- Prepare them for a CBRN incident.
- Provide security advice for staff and customers during such an incident.
- Manage the scene till the arrival of dedicated services.

This report provides recommendations for procedures for acting before, during, and soon after the CBRNe incident. These are universal rules for sites that are particularly vulnerable due to their characteristics.

This guideline aims to reduce the risk of a terrorist attack and limit its consequences. Terrorists can both identify and exploit weaknesses in the security system, which is why the information contained here will help to identify weak and potentially dangerous points that should be paid special attention to so that joint efforts have a positive impact on the safety of their employees and customers in general and VIP in particular.

For the information contained here to be complementary, it is necessary to familiarize yourself with other safety content supplemented by professional training as well as practical training.

The recommendations provided here must be compared with the country law as each EU country could have specific laws, and regulations while each hotel or hotels chain has its own best practices.

This report contains:

- General information.
- Description of CBRN detection and protection technologies and equipment that could be used to minimize the effect of CBRN incidents.
- A general, structural approach to minimize the risk of CBRN incidents as well as specific practical procedures for prevention and response to it.
- Recommendations and guidelines for improving CBRN security.

Because VIP visits are extremely sensitive and many times involve a great degree of

confidentiality, the level of threat in this type of event is increasing. For this reason, the special procedures and solutions for this type of event need to be elaborated.

Although in terms of security attributions we can subdivide VIPs into the three different levels mentioned below, for the purposes of this document, the terminology used to define these personalities will always and only be VIPs.

- Top rank VIP: personalities entitled to permanent police protection and who are most often government representatives. In these cases, the HCCs host the spaces and collaborate with the guidelines requested by the protection services.
- Very VIP: personalities with permanent personal protection by private (non-police) security, usually celebrities and businessmen. The security to be implemented is defined in accordance with the specific personality's protection services, and may vary according to their specific needs and requirements.
- VIP: personalities who are not usually under permanent private security protection, but who may be given this protection at specific times. They are usually important people for various reasons, but who do not fit into the two previous points. In these cases, the measures to be applied in the HCC will be defined in close collaboration between the security services assigned and those responsible for the HCC.

In terms of the type of protection, the terminology of active security or passive security can also be used. Active security is when security is provided by VIP security in consultation and collaboration with the HCC, and passive security is when security is provided only by the services already in place at the HCC.

To achieve the main objective of creating a CBRNe VIP protection programme, we intend to develop the following tasks:

- Communication procedures and practices between all security stakeholders
- Prevention procedures.
- Detection procedures.
- Reaction procedures.
- Creation a negotiating protocol in case of CBRNe VIP event.

The aim of these procedures is supporting the HCC community for prevention, detection and reaction to a CBRNe threat or event.

Prevention procedures

The prevention is the first step to avoid a terrorist attack and this chapter addresses and lists the importance of procedures related to preventing CBRNe threats. The prevention rules, policies and procedures resulting from them are in general not VIP specific. However good prevention makes each further security stem more robust and easier.

Creating risk awareness and security culture are keys to making HCC safer spaces. Defining, promoting**,** and making security policy a corporate responsibility is the cornerstone on which all the next elements are set.

It is important that you make and understand the security plan and your role within it, and that you and your staff understand their roles and responsibilities with proper assignment, and systematic participation in training and exercises. By carrying out a risk assessment, you can assess whether adjustments to your security plan are necessary.

It is difficult to overestimate the role of prevention. Only proper preparation for a potential attack will allow for its effective counteraction. Properly securing the object against attack is a factor that discourages attackers. They will tend to attack another, unprepared place. In an attack situation, there is no time to think about the best way to respond. Schemes of protection against the attack and reaction to it must be prepared and tested in advance.

Implementing effective procedures for person verification and luggage searches in HCC is crucial for ensuring the safety and security of guests, staff, and the premises.

Here are some best practices for conducting person verification and luggage searches:

- Establish Clear Policies and Procedures: Develop comprehensive policies and procedures for person verification and luggage searches, outlining the objectives, scope, and guidelines for conducting these activities. Ensure that all staff members are trained on these procedures and understand their roles and responsibilities.
- Utilize Access Control Measures: Implement access control measures, such as key card systems, security checkpoints, and designated entry points, to regulate access to the premises. Restrict access to authorized personnel and guests, and monitor entry and exit points for suspicious activity.
- Screening of Guests and Visitors: Require all guests and visitors to provide valid identification upon check-in or entry to the hotel. Verify the identity of guests using government-issued photo identification documents, such as passports or driver's licenses. Use electronic verification systems, if available, to authenticate identification documents.
- Train Staff in Observation Skills: Train front desk staff, security personnel, and other relevant employees in observation skills to identify suspicious behaviour or indicators

of potential threats. Encourage staff to be vigilant and report any unusual or concerning activity to security personnel or management.

- Implement Baggage Screening Procedures: Establish procedures for screening guests' luggage and belongings upon check-in or entry to the HCC. Use X-ray machines, metal detectors, or manual inspection techniques to detect prohibited items or suspicious objects. Clearly communicate these procedures to guests and ensure they understand the reasons for the screening.
- Deploy Technology Solutions: Invest in technology solutions to enhance the efficiency and effectiveness of person verification and luggage searches. This may include the use of electronic ID verification systems, biometric authentication technologies, and advanced baggage screening equipment.
- Coordinate with LEA: Maintain open lines of communication with local LEA and collaborate on security initiatives and threat assessments. Seek guidance and support from law authorities for implementing best practices in person verification and luggage searches.
- Regular Review and Evaluation: Conduct regular reviews and evaluations of person verification and luggage search procedures to identify areas for improvement and ensure compliance with industry standards and regulations. Solicit feedback from guests and staff to assess the effectiveness and efficiency of security measures.
- Stay Informed About Emerging Threats: Stay informed about emerging security threats and trends in the hospitality industry, including new techniques used by criminals to circumvent security measures. Adapt person verification and luggage search procedures accordingly to mitigate evolving risks.

By implementing these best practices, HCC can enhance their security posture and create a safe and secure environment, not only for VIP, but also for guests, staff, and visitors.

4. Measures to be implemented by the management

- Make security everybody's matter of interest and responsibility
- Formulate security policy, and have it announced to all staff
- Assign roles and responsibility areas
- Establish permanent mechanism for vulnerability detection and threat receptibility
- Establish communication loops for security important information flow
- General framework for cooperation between HCC, local security and VIP bodyguards-security: Scope, limits and exclusion areas. If VIP is not individually protected, LEA takes place of individual VIP protection.

5. Measures to be implemented by the local security officer

HCC managers must implement basic space control measures.

The implemented measures and PPE must be standard, the same and defined according to specific place. If you are staying overnight, they must be maintained continuously throughout the night. If it's during an event you have to use the general measures defined by the hotel or conference centre, unless you have security or individual protection who will give you the necessary support.

The measures and PPE must be defined in a standardised way and according to the specific facilities, in order to create routines in their implementation, whether for a regular customer or a VIP. They must be maintained for the duration of the visit, if necessary with continuous monitoring during the night. In the case of large events in HCC, the general measures defined by the respective space and event must be implemented, except in the case of VIPs who have security or individual protection that will give them the pre-defined protection for the specific case.

Space and access control procedures and good practices:

1. Observe customer behaviour, be aware of suspicious persons - remember appearance does not indicate intentions and it does not necessarily have to be the one person (e.g. look out for accomplice(s), people dressed unusually (long-sleeved shirts or coats on warm days) wearing protective masks (outside of pandemic time)).
2. Pay attention to luggage being carried in.
3. Pay attention to items left or unattended.
4. Report relevant safety observations to the next level.
5. Inform security in the HCC of suspicious incidents.
6. Do not obstruct escape routes and exits.
7. React strongly to any attempt to breach security areas.
8. In case of a change of employee, immediately cancel access to the area for the card in question.
9. In the event of theft or loss cards, replace or re-verify cards.
10. Keep keys to sensitive areas in the security room.
11. Change the access code periodically.
12. Control entrances from technical/storage areas.
13. Sensitize staff about information security.

Staff training on hazards and emergency response procedures:

1. Facility training including emergency exits and evacuation plan, location of first aid kits, location of necessary firefighting equipment.
2. Periodic training and drills regarding general safety and CBRN:
   - Searching the rooms for any left-over dangerous items, packages, luggage.
   - Premedical first aid.
   - How to behave if there is a possibility of contamination of the place where the employee is located.
   - Evacuation of customers and employees.

Essential Personal Protective Equipment

Equip the workplace with the necessary PPE:

- Protective masks (FFP3, escape hood).
- Disposable gloves.
- Disposable coveralls (for thermal protection if needed).

Remember it does not cost much, but you can gain a lot (consider additional protection measures).

Technical safety measures

Invest in technical measures that make your workplace safer:

- First aid kits.
- Cameras.
- Anti-panic remote controls.
- Access control system.
- Burglar proof doors.
- Emergency light source (torch).
- Chemical light (red, green).
- Power Tape.
- Large waste bags.

Figure 2 Example of first aid kits available in hotel

Source: https://esoftskills.com/hospitality/managing-and-training-for-emergency-situations-in-hotels/ Access: [05.2024]

6. Safety systems

Monitoring all activities in HCC public areas is crucial to maintaining order and overall control over the facility. The possibility of a particular building becoming a terrorist target is generally difficult to predict. Consequently, there is no specific pattern to determine the level of risk for a particular building.

No building can be fully protected against a determined individual who intends to disperse a CBRN agent. However, facility owners and managers can turn their buildings into less attractive targets by reducing the vulnerability to a CBRN attack. This can be achieved by putting in place appropriate deterrents, detection measures to prevent the attack from taking place, slowing it down and by putting in place response plans and procedures to mitigate the effects of their release.

Decisions on what security measures should be applied to a building should be based on several factors. These are primarily based on the estimated risks associated with the facility and its customers, the technical and architectural feasibility, and the costs incurred to introduce or modernize them.

Some of the systems and solutions for HCC include:

- Closed-circuit television system.
- Ventilation and fire protection systems.
- Access control system.

Security and safety systems are a whole set of technical measures that can be used to protect against a terrorist attack using CBRN agents, but also to minimize the consequences of their use.

6.1. CCTV

In the digital age, video surveillance has become the most valuable factor in providing security in public areas.

Most HCC install CCTV systems to monitor common areas such as entrances, front desk, pavements, walkways, emergency exits and car parks. CCTV provides excellent image quality and provides security departments with a clear picture of the installations in real time and recordings.

Extremely important places that should be monitored are technical corridors and evacuation

corridors and staircases. This will enable better and faster recognition of potential danger. It will enable better management of potential evacuation and search for potential victims who may be there.

State-of-the-art CCTV systems with advanced facial, abnormal behaviour, monitoring and left-object recognition functions are already available and implemented in many locations. Innovative software solutions used create previously unattainable opportunities for detection and notification in the event of a potential CBRN terrorist attack or other hazardous event.

6.2. Access control

Access control systems are responsible for physically preventing an intruder from gaining access to protected premises.

Access control is an important element in the physical protection of all facilities in general. It provides continuous protection, security for people, assets and sensitive information. Access control can be a simple or complex system, depending on the estimated threat to the facility.

Access control is a common way of checking people, namely to limit access to reserved areas. Increasingly, systems for voice or fingerprint verification are being used, which dramatically improves security, especially in sensitive areas of the facility such as security, monitoring or management offices.

The main components of the access control system are as follows:

- Security tokens (electronic ID card or biometric identifier, e.g. fingerprints).
- Card readers (at access points).
- Decision-making element (processor or computer).
- Output (alarm signal used to inform in the event of unauthorized access powering the door lock, signal to cameras to take a picture when entering, barriers or other devices).

Some of the benefits of using an electronic access control system are the follows possibilities:

- Connecting to doors that are electrically powered, thus preventing unauthorized access.
- Collect and store all the data concerning persons who have gained access (person, time and place).
- Integrating with a CCTV system to increase the efficiency of access control.

- Integrating with an alarm system that will alert security in the event of a security zone breach.
- Opening any door to facilitate evacuation in a CBRN or other emergency event.

7. Security searches

Conduct a search operation

The security manager should decide whether to search or not to search. If there are any indications that information about a CBRNe attack is true, it is recommended that an evacuation should be carried out under the rules in the evacuation section and the security services should be notified immediately.

Security personnel familiar with the topography of the facility, with the means of communication, and with the knowledge necessary to search safely should be selected in the first instance.

If it is decided to use technical staff, cleaning service, or office administration to search the premises, they should be familiar with the situation and trained to carry out such activities.

The facility should be divided into zones:

- Zone 1 - Outdoor zone (car parks, litter bins, lawns, hot spots, etc.).
- Zone 2 - Internal and accessible to customers (communal spaces, reception, toilets, circulation routes, lifts, escape routes, etc.).
- Zone 3 - Internal and not accessible to customers (technical spaces or installations, offices, back rooms, delivery zones, etc.).

Rooms should be searched in teams of two as far away from each other as possible. Begin the reconnaissance by listening for suspicious sounds. Then carry out visual reconnaissance (avoid opening, and moving objects). Carry out reconnaissance at several levels and in a structured manner (Figure 3).

- From floor to hips.
- From hips to head.
- From head to ceiling.
- Technical spaces and suspended ceilings.

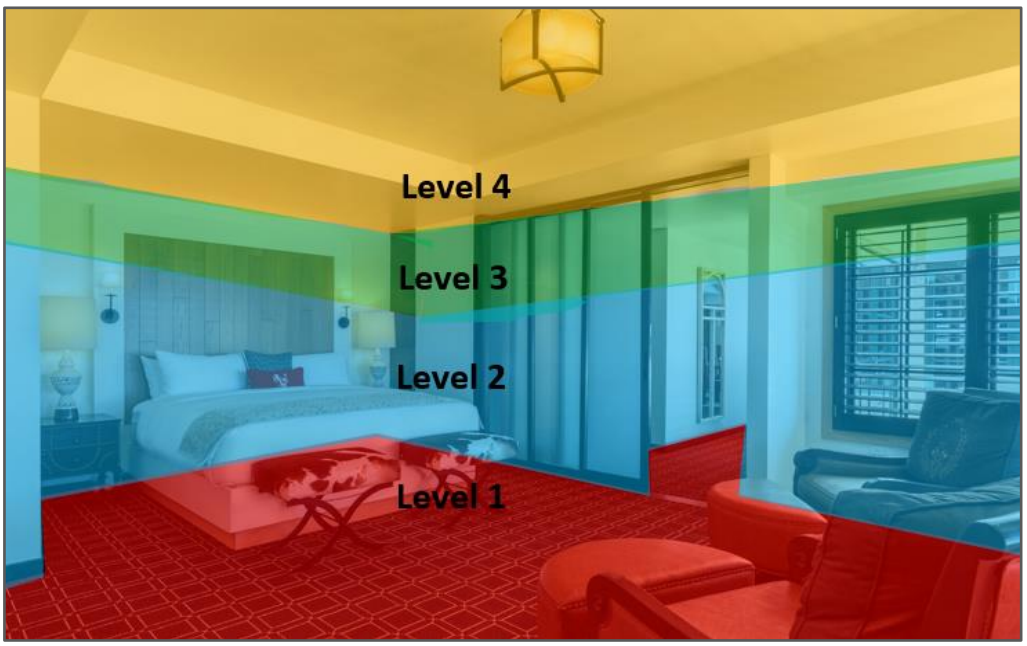

Figure 3 Example of search levels zones

Source: Own source

Mark the rooms searched so that activities are not duplicated by other search teams or security services.

A search manager should be assigned to each area, who should coordinate activities and pass information to the person responsible for the security of the facility at any given time.

Searching individuals should:

- Be trained in conducting search operations.
- Always consider the worst-case scenario and be aware of the danger.
- Do not be afraid to report a threat - only a quick response will minimize the effects of any CBRN agent.
- Always update your status through available means of communication (communications, mobile phones, mobile messengers, etc.).
- Carry out activities in accordance with your equipment and your own knowledge of the field.

What should be sought:

- Anything that should not be in a particular place (left-over objects, suitcases, backpacks, bags, barrels, containers, etc.).

- Anything which cannot be explained by its presence.
- Anything that is not in its place.
- Anything that resembles artillery ammunition, explosives, spectacle pyrotechnics.
- Objects containing clocks (mechanical or electronic), radio devices with protruding electric wires, detonators, etc.
- Objects leaking an unknown substance, emitting smoke, making noises.
- Objects attracting attention by their external features (eye-catching, inviting to be picked up).
- Overloaded vehicles, vehicles without number plates (with reported stolen plates, inconsistent front to back).
- Vehicles with darkened windows, making it difficult to visually inspect the contents of the car.
- Unusual smell, incompatible with the environment, sharp, unpleasant, irritating, suffocating.
- Chemicals products, laboratory equipment.
- Vehicles and packages marked with stickers or information plates in accordance with the ADR (Carriage of Dangerous Goods).
- PPE (acid-resistant gloves, aprons, gas masks, safety goggles, protective clothing, etc.).
- Bright stains.
- Corroded, rusted metal.
- Dead animals in the area.
- Dead or missing insects.
- Unusual dead vegetation.

When any hazard is noticed, move away to a safe distance, start reporting and informing, then follow the procedures in the safety instructions. Always assume the presence of secondary threat/devices.

<u>What not to do:</u>

- Do not touch, move or carry the suspect object to another location.
- Do not cut or sever any cables, cords, wires, or other connecting items.
- Do not alter natural or artificial light sources.

- Do not smoke, do not use open flames.
- Do not switch anything on or off.
- Do not taste anything.

Any security search during VIP visit will be conducted by their security service and according to their rules. To avoid leaving any gaps, HCC and the external agencies should agree scope and timing of the search.

8. Special dedicated Personal Protective Equipment

In this chapter, the report present the importance of PPE for self-protection.

The most important categories of PPE, like eye protection, respiratory protection, skin protection is discussed shortly. Rules and factors influencing proper selection of PPE are depicted.

In the final part of this chapter we recommend use of:

- Full face gas mask for managing staff (security and staff management).
- Escape hoods for VIP and people controlling evacuation.
- Protection gloves also for people controlling evacuation.

8.1. PPE description

PPE is individual, specialized equipment and clothing that will provide protection against hazards (e.g. chemical agents, infectious agents and toxins).

General work clothing (such as coveralls, trousers, work shirts) are not considered as PPE. There is a range of clothing available to protect against CBRN agents.

The use of the specific PPE required is determined by a risk assessment, while to counter the effects of a terrorist attack with CBRN agents, the aim should be to protect as effectively as possible against all possible scenarios.

When selecting appropriate PPE, size is a very important criterion. Choosing the right size of equipment ensures that its properties are maintained. Further factors influencing the effectiveness of protection are the use of compatible PPE (masks, goggles, suits, gloves), proper fitting and sealing of the connections so that they form a tight unit, proper training in dressing and undressing.

8.2. Eye protection

They should provide eye protection against chemical and biological splashes and protect against dust. Structurally, goggles have shields on the sides to prevent these substances from entering the eye in angled splash situations.

Safety glasses do not provide full protection against dusts, vapours and aerosols entering the eye, so the use of suitable protective goggles is recommended despite they are less comfortable and little training is needed.

Very often eye protection is integrated with face masks, which provide the best protection. Goggles made of soft components that provide a tight fit with a suitably curved surface to fit the face work best.

In case of VIP see 5.1.2.2 Respiratory protection.

8.3. Respiratory protection

Respiratory protective equipment is used to protect personnel from inhaling airborne hazardous substances and materials in various forms (aerosols, liquid/solid particles, gases or vapours). There are a number of possible hazards associated with respirators, which must be borne in mind in order to avoid them:

- Incorrect fit and wearing of respiratory masks - a mask cannot fully protect if it's size in not proper and the seal between mask and facial skin is leaking
- Touching the inside of a respirator mask (which traps viruses etc.), can result in the transfer of contamination and eventually lead to substances entering the mouth and nose.
- Taking unnecessary risks of exposure for respirator wearers, as a result of a false sense of security; it is always safest to keep a distance, an appropriate distance from another person or hazard zone.
- If the threat is unknown (agent or agents concentration level is unknown) only system with independent air (SCBA system with compressed air in a cylinder) has to be used to enter the contaminated zone, other system could be used only for evacuation).

There are three types of respiratory protection (forced-circulation filtering masks):

1. Air Purifying mask.
2. Filtering half-masks.
3. Full-face masks.

These devices filter the air of hazardous substances. The use of a particular solution depends on the air quality in the environment.

They can only be used when the oxygen content is at an appropriate level (minimum 17%) and the type of hazardous substance is known (only the correct filter used ensures correct functioning). It is therefore advisable to use masks with filters with the widest possible spectrum of action.

The following protection measures can be distinguished:

1. Disposable respirators/dust half-masks

   Recommended filtration class FFP3/P3/N99/N100 - they do not provide protection against chemical substances in gaseous form, and are mainly used when the hazard has a form of particulate matter in macro scale, is solid / liquid aerosol or suspension , such as bacteria, viruses, dust carrying radioactive material, pathogenic and fungal spores and aerosols (except aerosols of chemical substances with a vapour pressure at ambient temperature giving concentrations above the safety limit).

2. Partial masks

   Half masks with replaceable filters - depending on the filters used, provides a good respiratory protection solution for most CBRN hazards.

3. Full-face masks

   Provide respiratory and eye protection at the same time, available in single or dual-filter versions:

   - Isolation or self-contained breathing system - mainly used in areas where the oxygen content is below 17% or where there is a dangerous concentration of hazardous substances. This solution provides a constant supply of air or oxygen and is a self-contained breathing apparatus. When used correctly, it provides full protection against the effects of CBRN agents. The equipment requires periodic technical inspections and personnel using it must undergo appropriate medical examinations and training.
   - Escape - these are used in emergency situations to provide immediate protection from harmful agents for a limited period of time.

4. Escape hood with air filtering canister

There are:

1. Ambient air-dependent devices.

   These are fire and escape hoods with efficient filtering devices installed, designed to

protect against toxic gases, vapours and industrial and fire particles, ensuring adequate filtering for a period up to 15 minutes; this type of device is dependent on ambient oxygen.

2. Equipment independent of ambient air:
   - Compressed air apparatus - these are systems that provide a continuous supply of air for a minimum of 15 minutes from a compressed air cylinder, and come in the form of a full-face positive pressure mask or escape hood
   - Regenerative breathing apparatus - providing access to oxygen in toxic gas conditions and in the absence of oxygen in a given environment; depending on the version, they provide air supply for up to 60 minutes.

8.4. Protective gloves

They are an integral part of protection for the overall security management staff. They should be used whenever a CBRN incident is suspected. They must meet a number of requirements as should be resistant to chemical, biological substances. For those doing manual jobs they should also be resistant to abrasion and other damages, thin enough not to impede manual activities. Their selection is therefore crucial to ensure adequate protection for the worker. By design, double-dressed pairs of gloves should be used during CBRN incidents.

This serves primarily to protect against cross contamination when undressing after decontamination, in addition to providing additional protection against damage to the top protective layer.

The most versatile and protective gloves are nitrile protective gloves with a thickness of 0.2 - 0.4mm, which have adequate chemical and biological resistance, mechanical resistance, anti-static properties and do not significantly impede manual activities. Note: latex gloves don't provide protection against chemical or biological hazards.

8.5. Protective clothing

Protective clothing provides a barrier between harmful external agents and the human skin. Depending on the application and the risk, it is divided into categories. There are several classifications of protective clothing. The one presented below is made for being used in these Guidelines.:

- Category I – Minor risk: Providing protection against minimal risk.

- Category II – Intermediate risk: Providing protection against medium risk, specific factors not endangering life and health.
- Category III – Major risk: Serious or mortal danger, representing protection against external factors endangering life and health.

The suits of the highest category of resistance, are divided into six subcategories (type 1-6). They are made of materials that provide adequate chemical and biological protection and are lightweight and comfortable. The most versatile suits for non-professionals are those providing protection against pressurized liquid jets and biological agents. Additional equipment includes shoe covers or over boots and an integrated protective hood. In order to ensure adequate protection, it is essential to have the right size, and be trained in dressing and undressing.

- Type 1 (EN 943 standard): Gas-tight chemical protection suits, protecting against liquid chemical agents, gas and aerosols as well as very fine particles. They are equipped with a breathable air supply inside the suit (type 1a) or outside (type 1b) via an air supply system.
- Type 2 (EN 943 standard): Non-gastight garments, protection against chemical products, liquids and aerosols.
- Type 3 (EN 14605 standard): Chemical garment, resistant to liquids in the form of continuous jets.
- Type 4 (EN 14605 standard): Fogs and liquid sprays tight coverall.
- Type 5 (EN 13982-1 standard): Protection against solid particles suspended in the air.
- Type 6 (EN 13034 standard): Limited time protection against liquid chemical splashes.

Figure 4 The Signs and Symbols for PPE

Source: EN ISO 13688

9. PPE recommendations

Different agents classes (C, B or RN) require different protection systems. For instance for B agents and radiation emitting particles efficient filtration against particles is enough to protect respiratory system. So FFP3 mask will be good enough to significantly reduce threat from B agents. It could also reduce contamination risk from radioactive dust, especially vs radioactive materials emitting alfa, beta or radiation, but not vs chemical agents. On the other hand masks with gas filter could absorb toxic gases and also filter out bio or radioactive particles. Recommendations provided below do not require identification of threat class (C, B or RN) as it could be not possible at the moment of CBRN attack or incident.

Please keep in mind that protection vs radiation proposed below is focused on inhalation of active particles or radiation gases only. There is no efficient PPE vs radiation.

There are only 3 ways to reduce radiation threat:

1. Distancing – stay as far as possible from the radiation source (run away).
2. Timing – reduce exposure time (in short words - run away).
3. Shielding – put some material absorbing radiation between a radiation source and exposed person – shielding potential is characterized by own attenuation factor which is a characteristic property of every material.

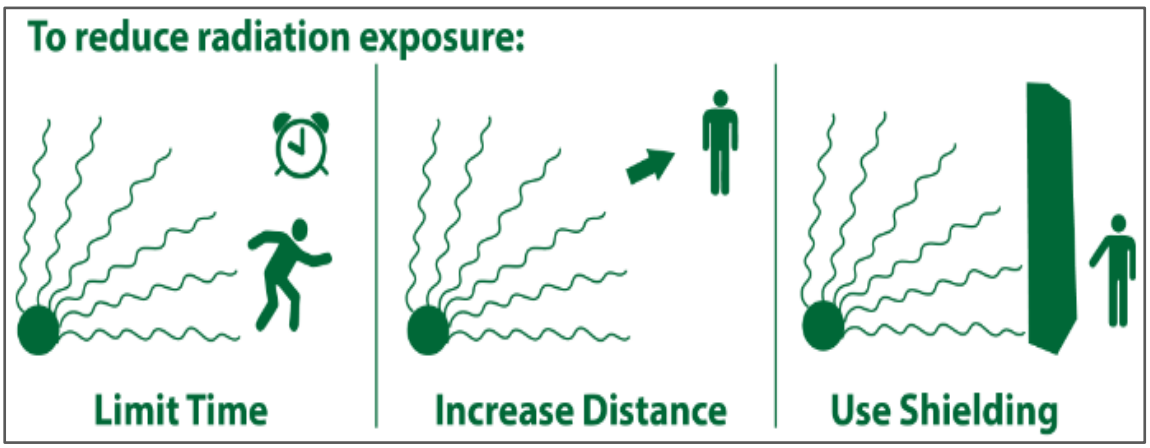

Figure 5 Reduce radiation exposure

Source: Based on www.epa.gov/radiation/protecting-yourself-radiation [Access: 04.2024]

Requirements for CBRN PPE:

- Simplicity – to make use of it easy.
- Universality – to protect a person against all CBRN agents classes.
- Low purchasing cost.
- Low maintenance cost.
- Protection long enough to perform intended action (escape or manage the scene).

9.1. Escape Hood

This type of protection is recommended for escape from danger zone or through contaminated zone if there is no other way.

It could also be used to rescue a person which is trapped and is using shelter-in-place procedure.

Features:

- Simplicity – it takes seconds to don.
- Universality – provide protection versus all CBRN agents classes.
- Low cost of purchase.
- No maintenance needed.
- Shelf live: 5 years.
- Protection time: 30 minutes.

Figure 6 Escape Hood (ScapeCBRN30)

Source: Own photo

9.2. Victim Rescue Unit +

This type of protection is recommended for escape from danger zone or through contaminated zone if there is no other way.

It could also be used to rescue a person which is trapped and is using shelter-in-place procedure.

Features:

- Simplicity – it takes seconds to be done.
- Universality – provide protection versus all CBRN agents classes.
- Low cost of purchase.
- No maintenance needed.
- Shelf live: 10 years.
- Protection time: up to 60 minutes.

Figure 7 VRU+ (Essex Industries)

Source: https://essexindustries.com/products/victim-rescue-unit-plus-vru/ [Access: 04.2024]

9.3. Gas mask

This type of gas mask could be used vs different CBRN agents and if case of nearby chemical plant or chemical storage facility dedicated gas filters could be used.

This is PPE dedicated to security staff or managers it allows to maintain high mobility in crisis situation (managing evacuation, checking places).

Features:

- Simplicity – it takes seconds to be don (short training needed).
- Universality – provide protection versus all CBRN agents classes.
- Moderate cost of purchase.
- Low maintenance needed.
- Shelf live: mask: 10 years, gas filter – up to 5 years.
- Protection time: up to 24h (depending on gas concentration, gas filters could be changed in contaminated area).

Figure 8 Gas mask C50 Avon with filter AVEC

Source: Own photo

9.4. Protection gloves

Nitrile gloves

Any nitrile gloves provide good temporary protection vs different chemicals.

The thicker the longer protection time and lower puncture risk. For better safety user can wore two gloves one on another. It is strongly recommended not to touch anything in contaminated area, but sometimes user has to open the door or touch access pad.

This equipment is recommended for security officers, managers or any of the staff having roles for instance during evacuation.

Features:

- Simple to use - short training needed especially for removing step.
- Very low cost of purchase.
- No maintenance needed.

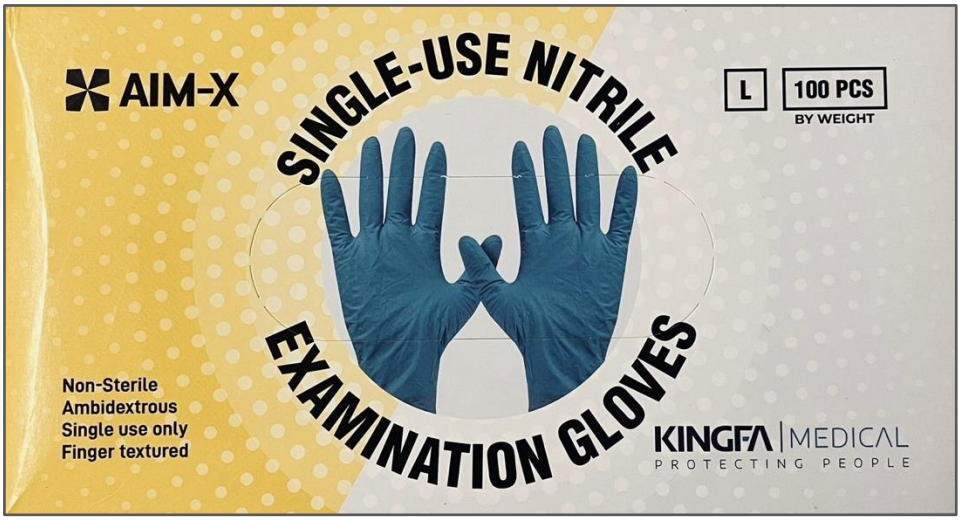

Figure 9 Nitrile Gloves

Source: Own photo

9.5. Protective clothes

Protective clothes are type of equipment which is worn only by those who need it e.g. having roles in managing evacuation. Putting on protective clothes needs time. If a user puts on protection clothes in a hurry it can lead to false protection confidence. Moreover, if there is no decon station deployed and no one can help taking off these protective clothes it can lead to cross- contamination.

So, it is better to run away faster than spend time on wearing protective clothes.

We recommend:

- Use of escape hoods (or VRU+) especially for VIP and people controlling evacuation.
- Full face gas mask – for managing staff (security and staff management).
- Use of protection gloves – for people controlling evacuation.

9.6. Recommendations for VIP PPE

VIP are supposed to escape the incident site as soon as possible. For that reason for the sake of rapid reaction and simplicity only respiratory tract and hand protection are required. For respiratory protection an escape hood equipped with compressed air cylinder is recommended to use by VIP in case of a suspected or real emission. When the hood is used, eye protection is not necessary. Double layer of nitrile gloves are sufficient to provide hand protection during the escape.

10. Special communication procedures and protocols with LEA

Due to the nature of an incident involving CBRN agents, adequate information and notification are very important elements.

Persons without specialized equipment and training should not be directly involved in providing first aid and countering the effects of these agents. Therefore, always emphasize the nature of the incident when informing and notifying, so that those responsible for coordinating the alert and notification activate the appropriate resources, adapted to respond to such incidents. It is crucial, in response to CBRN incidents, that the relevant (specialist) services are notified of the nature of the incident. Otherwise, units not prepared for this type of action will be dispatched to the scene, which may result in additional casualties and loss of time necessary to provide first aid and initiate decontamination procedures. Therefore, facility security, management, and staff should be trained in proper information and notification.

Good information management and efficient notification are key elements when it comes to HCC security. Information management as well as notification should start with the corporate management culture. This is where the direction and level of security procedures and rules should be set and implemented, which directly translates into the ways, methods, and scope of notification and information in the area of security at individual HCCs. Please note that VIPs are always come with own security and direct communication between hotel staff and VIP security must be established, especially informing about existing vulnerabilities, suspicious items, people or behaviours should be reported to VIP security staff.

There is a subtle difference between notifying and informing the definitions given below distinguish not only the area and time of the information provided but also indicate how to proceed once the information has been received.

1. Information - is understood as the distribution of messages about how to mitigate risks, what to do in the event of a risk turned to be an incident, , including the possibility of obtaining assistance to deal with the consequences of the risk. (Mostly prevention or reporting).
2. Notification - the communication, by all available means, of specific information to alert the competent authorities and the population to the possibility of a hazard, its occurrence, or its cessation, and to provide information on how to deal with it. (Emergency response).

Information

In the case of HCC, we can distinguish between different lines of information dedicated to specific audiences and carrying different information content:

Internal:

1. Dedicated to HCC staff and superior management units - regarding:
   - Changes in security procedures.
   - Changes related to the organization of the facility.
   - Information on potential risks.
   - Information on possible disruptions such as power cuts.
   - Implementation of new systems affecting security.
2. Dedicated to customers - in terms of:
   - Evacuation.
   - Security in areas inside and outside the facilities.
3. Dedicated to security or decisionmakers

External:

1. Dedicated to VIP security
2. Dedicated to emergency services - in terms of:
   - Training and training needs.
   - Needs related to content and practical support during occasional events.
   - Adaptation of systems to the needs of services in emergency situations.
3. Dedicated to cooperation with industrial plants posing a potential risk in the event of an accident, natural disaster, or terrorist attack.
4. Dedicated to cooperation with the authorities supervising the transport of dangerous goods in the vicinity of an HCC.
5. Dedicated to HCC organizations - in terms of:
   - Communication of potential threats including - threats, extortion attempts, and intimidation.
   - Effective solutions and practices developed that have a significant impact on improving security.
6. Dedicated to the wider public in terms of informing the media about the situation and actions taken after the occurrence of crisis events.

7. Dedicated to the city's crisis management institution.

Notification

In critical situations, it is advisable to have an emergency notification plan to facilitate prompt and timely communication. Often, it is the facility manager who must take responsibility for managing communications in the event of an unwanted emergency in their HCC.

As with information, notifications can be divided into two groups and dedicated to particular target audiences:

Internal (responsibility of any member of staff, who must report to their immediate superior whenever they notice or suspect anything unusual on the premises):

1. Dedicated to HCC employees, security services, customers, and superior management units - in terms of:

- Notification of the occurrence of an emergency within the limits of the facility (see EVACUATION ANNOUNCEMENT).
- Actions necessary to minimize the consequences.
- Actions necessary to remove obstacles occurring during evacuation operations.
- The coordination of security activities.
- Organization of the work of the emergency response team.

External (responsibility of facility or security manager):

1. Dedicated to the emergency services - in terms of:

- Alerting of the occurrence of the event (see METHANE protocol).
- Notifying emergency services of the state of the situation upon their arrival on site.

Various forms of information and notification are used to effectively reach the designated beneficiary groups and make use of both technical and traditional means:

1. Information signs and instructions.
2. Digital radios - treated as the main or backup communication between the administration, staff, and other employees.
3. GSM communication - as the primary communication with customers, external entities, and emergency services using GSM technology. This solution guarantees fast access to selected customers but has the disadvantage of losing connectivity if base

stations are overloaded, usually in case of emergency events.

4. WI-FI communication - guarantees a stable connection between the people involved but only within the boundaries of the facility.
5. Telephone communication - wired communication so-called "hard link" is the most stable type of communication, least exposed to external factors, and used most often to maintain communication between key elements of safety management in a HCC.
6. VAS - voice alarm system - according to fire regulations. Is a mandatory system for announcing warning signals and voice signals for the safety of all persons within the boundaries of the facilities.
7. Communicators - WhatsApp, Signal, etc. Applications are used to group recipients by segments, such as location or type, so they can be notified of events or critical situations that affect them.
8. E-mail - mainly used to share experiences, communicate changes that have occurred, or report on historical events.
9. Sirens and alarms.
10. Dedicated applications:
    - Applications of this type provide the opportunity for rapid, two-way emergency notification to management, security, staff, and customers.
    - Applications for people with disabilities.

It should be emphasized that a well-designed and structured notification and information system must be combined with training and drills for customers as well as for HCC staff. An example would be the procedure for creating a safe place from the effects of a chemical agent attack. Through an app, customers can be instructed to implement a shelter-in-place procedure, but without prior training, this will not have the desired effect.

It is recommended that customers are informed of the general level of national as well as local security, which will influence their situational awareness as well as the possible manner and speed of response to a real threat. Facility managers should not be afraid to use all staff to observe or disclose dangerous situations or objects within their premises and the HCC. Such staff-customers cooperation can only be beneficial and will improve safety.

Recommendations

For the security system to operate efficiently, it is essential to obtain information quickly and efficiently and to transfer it further, therefore following solutions are recommended:

1. Equipping security staff with encrypted radio communications based on digital radios to exclude external interference of the information stream.

2. Providing the HCC with comprehensive radio signal coverage, with transmitters and signal amplifiers.
3. Organizing alternative communications (e.g., own WiFi network, which will enable the efficient transmission of information to the mobile phones of HCC staff).
4. Securing additional sim cards from other GSM network operators than those used on a standard (daily) basis.
5. The implementation of a smartphone app in the HCC for quick contact with customers and staff. Apps of this kind offer the possibility of rapid two-way notification of threats to all authorized access groups.
6. The use of mobile applications that make it possible to notify people with verbal communication difficulties (people with hearing impairments) in a graphical way (e.g. the Alarm 112 application).
7. Preparing a list of the most important emergency telephones for security services, including those responsible for CBRN security in your area.

Below is an example of the chain of notification of a hazardous incident, together with the responsibilities and activities of the position.

Basic behaviour of HCC functionaries according to their position in the security management chain:

First line security, HCC technical staff:

1. Situation recognition:
   - Where (exact location of the incident).
   - How many persons affected.
   - The nature of the incident (e.g. unconscious, vomiting, strange chemical smell).
2. Transmission of the above information to the security manager (or person in charge of security).
3. Securing the area to prevent unauthorized access.
4. Secure themselves with available personal protective equipment (e.g. gloves, masks, goggles).
5. If possible, pull injured persons out of the hazardous area following safety procedures. Such action is only possible if:
   - There is a certainty that there is no immediate danger to the responders.
   - The responders have appropriate PPE for the hazard.

Monitoring personnel:

1. Situation recognition - analysis of recordings of incidents in the area (causes of symptoms and source of threat).
2. Monitoring the scene of the incident.
3. Informing and notifying security managers and emergency services.

Security manager/shift manager:

1. Analysing the situation.
2. Inform the HCC management of the nature of the incident.
3. Prepare for evacuation within their area of responsibility.
4. Informing the appropriate services about the incident and its nature.
5. Notify the emergency services indicating a suspected CBRN incident.
6. Supervising and coordinating the evacuation until emergency services arrival.

Management:

1. Analysing the situation concerning CBRN risks.
2. Notification of the relevant services of the incident and its nature.
3. Preparation for evacuation.
4. Decision on evacuation of the facility.
5. Supervision of the evacuation.

When informing and notifying the emergency services, it is important to indicate a safe access route and exit.

Dangerous item threat information:

Information on the planting of a dangerous item using a CBRN agent. Receiving a notification that a dangerous object has been planted, places a high psychological burden and can be a traumatic experience.

Therefore, the development of procedures and procedural training can enhance the incident management.

The information of the intention to plant or set off a dispersal/explosive device may be obtained:

1. By providing information by telephone.

2. By sending information by e-mail.
3. By mail or by dropping off in a conspicuous place (letter, postcard).
4. By dropping off a leaflet, piece of paper, for example in a toilet, corridor or other visible and generally accessible place in the institution.
5. Making a short inscription: with paint, lipstick on a window, toilet mirror, wall, etc.
6. It can also be a person who, while in the premises of an office or institution, announces that he or she has an explosive charge on him or her, in a briefcase or in his or her hands, and will detonate/disperse the charge if his/her demands are not met.

Information about a planted explosive device must be forwarded immediately to the staff responsible for security, to the management and to the Police.When interviewing a person reporting the presence of a dangerous charge, use a standard form, as the provided in the example below.

THREATENING INFORMATION FORM

1. Received call date (day/month/year):_____
2. Caller phone number: _____
3. The call was probably: ☐ cellular ☐ landline ☐ local ☐ long distance
4. Time: call start time:_____ call end:_____
5. Caller's sex: ☐ Male ☐ Female ☐ Minor
6. Caller accent: ☐ Native ☐ foreign language ☐:_____
7. Caller age (approx.): _____
8. Was the callers voice familiar to you?: ☐ No ☐ Yes: _____

Check for key words.

☐ Chemical	☐ Biological	☐ Radiological	☐ Nuclear	☐ CBRN
☐ Nerve	☐ Blister	☐ Choking	☐ Blood agent	☐ NBC
☐ Detonation	☐ Dispersion	☐ Explosion	☐ Liquid	☐ Gas
☐ Aerosol	☐ Acid	☐ Alkali	☐ Powder	☐ Detonator
☐ Fuse	☐ Initiation	☐ Trigger	☐ Switch	☐ IED
☐ Booby trap	☐ Bomb	☐ High explosives	☐ Trip wire	☐ Time delay
☐_____	☐_____	☐_____	☐_____	☐_____

9. **Information obtained (try to write down exactly what he said):**

_____
_____
_____
_____
_____
_____

10. **If possible ask questions (stay calm and polite):**

When it will be activated?:_____
Where is it planted?: _____
What kind of device is it?: _____

How does it look like?:_____
What is dangerous distance?:_____
What does it produce?:_____
What will cause when activated?:_____
Thank you, that you called. But why did you call?:_____
Who are you?: _____
Why are you doing this?:_____
What should I do?:_____

Try to hear the background noise:

☐ Traffic	☐ Voices	☐ Technical noise	☐ Trains	☐ Office
☐ House noise	☐ Silence	☐ Shopping mall noise	☐ Bar	☐ Street voice
☐ Siren	☐ Aircraft	☐ Kids	☐ public address systems	
☐ Animals	☐ Other:			

_____
_____

11. **How the caller behaved and spoke:**

☐ Aggressive	☐ Calm	☐ Emotional	☐ Rational	☐ Irrational
☐ Frightened	☐ Drugged	☐ Fast speaking	☐ Drunk	☐ Slow Speaking
☐ whispering	☐ Normal	☐ Rude	☐ Bot	☐ Recorded voice
☐ Other:				

_____
_____

12. Your personal data:

Name: _____
Position:_____
Time and date when completing the form:_____

Figure 10 Example of THREATENING INFORMATION FORM

Source: Own source

During a face-to-face or telephone conversation, demonstrate maximum calm and composure and seek to obtain as much detail as possible about the threat and the person providing the information. Any detail remembered from the conversation or an extension of the conversation may have a significant impact on the subsequent investigation.

Communicate the information obtained immediately to the HCC management, detailing the content of the conversation and the place, time and source of the information.

When completing the form:

1. Underline the relevant information.
2. Fill in during or after the interview simultaneously (recording if possible).
3. Keep the conversation calm and polite.
4. Pretend to have difficulty understanding the caller and try to prolong the conversation.
5. Make the caller aware of the possibility of causing, as a result of the attack, the death of innocent people who happen to be in the place where the device will be activated.
6. During the conversation, seek to obtain as much information as possible about the reporting party and his/her motives.

11. Detection procedures

In this chapter this report is focused on detection of the CBRN attack or incident. In the first part indicators and symptoms of such an event are listed to detect the thread without any additional equipment. This knowledge could allow faster reaction to the situation and could help organize early evacuation which is extremely important. Unfortunately, not always as some agents could be detected only by dedicated sensors. Requirements and recommendation for such equipment are delivered here.

11.1. Detection of CBRN attack/incident

There is a variety of possible methods of delivery CBRN agent to a victim.

Those methods could be as simple as just opening a container containing volatile agent, creation of leak, addition to water we drink or more complicated as creation a dispersion equipment or use of improvised explosive device.

It is extremely important how the agent is delivered, the same amount of specific agent could affect several or hundreds to thousands of people depending of way of delivery or route of exposure.

This is way in Chemical Weapons Convention (CWC) not only Chemicals Warfare Agents (CWA) are considered as a “weapon” but also means of its delivery.

Recognition of early stage of CBRN gives is extremely important for proper reaction and reduction of consequences of an CBRN attack or incident.

Effects of early detection are:

- Faster evacuation.
- Reduced exposure time.
- Reduced contamination concentration/doses which victim are exposed to.
- Reduced spread of contamination (fast ventilation stop, better control of contaminated people).

Which leads to:

- Lower number of victims.
- Lower severity of contamination (injury or temporary health effects vs long-term effects or death).

General differences in detection of C, B or RN agents are:

- **Time**
  - ✓ Effects of a C agent (a chemical) on person could be very rapid – symptoms could be fast and could be used for detection of attack.
  - ✓ Effects of B agent (bacteria, virus, fungi etc.) could be visible days after exposure – symptoms cannot be used for detection of B – type incident.
  - ✓ Effects of RN agents (radiation) could be visible weeks to months after exposure, unless source is extremely active which is very unlikely. There is no other option to detect RN agents than with use of proper detection equipment.
- **Persistence**
  - ✓ Some chemical agents may be persistent and contaminate the area for a long time, but majority react in environment or evaporate.
  - ✓ Biological agents sometimes create spore forms but in majority are destroyed in the environment, mainly due to UV radiation and reactions with ozone.
  - ✓ Persistence of radiation emitting elements depends only on the isotope type.
- **Dispersion and propagation**
  - ✓ Concentration of chemicals and toxins once released to the atmosphere only decreases with time.
  - ✓ Biological agents may multiply be transmitted directly or by vectors and create epidemics.
  - ✓ Radioactive substances may attract to dust which may propagate with air or water.

There are significant differences between C, B or RN agents which creates difficulties in early detection:

- Chemical agents: attack or incident where chemicals are involved are characterized by relatively fast observable effects (clouds, odours, droplets, dead animals etc.) or onset of medical symptoms (from minutes to hours).
- Biological agents: those agents are typically colourless and odourless and thus do not create characteristic signatures. Medical symptoms of attack could be observable in longer time (many hours to days or longer) which makes detection of an B incident more difficult. Additionally due to late detection affected area could be greater and control of affected people is very challenging. Bio agents can also have, which is unique among CBRN agents, ability to self-reproduction and creation of a bigger problem in time. Probably the only possibility to detect B attack is detection of the moment of the attack (strange aerosol dispersion, unusual cloud, low energetic explosion).
- Radiological or nuclear material: there is no possibility to detect radiation without detection equipment. Symptoms of exposure to radiation could be observed in days

to weeks or even much longer. Because of difficulty in detection possible contaminated area could be greater due to migration of contaminated people. The most probable RN materials or sources would not generate high enough radiation to kill or seriously injure people. In case of "dirty bomb" type attack primary hazard comes from explosion and it could be easily detected.

Below easy observable CBRN attack indicators are presented (ERG source):

Indicators of an C – type incident:

- ✓ Dead animals (birds, fish) – numerous dead animals of different kind (domestic, wild, small, big) in the same area.
- ✓ Lack of insects – if there is missing normal insects' activity (no sounds of insects, no flies or mosquitos) it could indicate presence of toxic chemical in the air. If the place is close to water check for dead fish or water birds.
- ✓ Strange odours – strange means not normal in the surroundings. Suspicious odour includes fruity, flowery, sharp, pungent garlic, horseradish like, bitter almonds, peach kernels, newly mown hay.
- ✓ Different looking area – dead weeds, bushes, trees, discoloured or withered leaves, crops.
- ✓ Unusual liquid droplets – surfaces are covered with oily droplets or film, water surfaces have an oily film.
- ✓ Mass casualties – high number of dead people or having health problems including nausea, disorientation, difficulty in breathing, convulsions, sweating, conjunctivitis, erythema, blisters, weals and/or rashes (see procedure 1-2-3+).
- ✓ Pattern of casualties – casualties distributed downwind, or if indoors, by the ventilation system.
- ✓ Illness in confined area – different casualties rate depending on the place of agent release (indoors vs outdoors).
- ✓ Low lying clouds – unusual, not expected in surroundings, clouds or smokes could be an early stage of release of agent. If improvised explosive device is used as a dispersion tool low energy detonation is very likely (in case of B or C - type attack) as strong explosion could destroy an agent.
- ✓ Unusual metal debris – unexplained bomb or munition material could be part of military equipment, especially suspicious if contains liquid.

Indicators of an B – type incident:

- ✓ Unusual number of sick people reporting to the health care institutions, increased number of deaths among humans or animals in the aftermath – different symptoms may occur. Casualties could occur hours to days after an incident. Time required for first symptoms to be observable depends on type of agent (see also procedure 1-2-3+).
- ✓ Unscheduled and unusual dissemination of spray – especially if outdoors during periods of darkness.
- ✓ Abandoned spray devices – devices which were used for an attack, they may have no distinct odour.
- ✓ Abandoned piece of PPE – Personnel Protective Equipment (used gloves, protective clothes).

Indicators of an RN – type incident:

- ✓ Radiation symbols – containers having radiation symbol on it.
- ✓ Unusual metal debris – unexplained bomb or munition-like material.
- ✓ Small, metal capsule (opened or closed) or small, dark metal like pellets.
- ✓ Heat emitting material – material that is hot or emit heat without any heat source.
- ✓ Glowing material – strongly radioactive material may emit or cause radioluminescence.
- ✓ Small but heavy package – to deliver safely strong radioactive source heavy lead container must be used.
- ✓ Sick people – not very likely scenario as radioactive source creating instant effects should be extremely active thus very difficult to obtain and deliver to the place (see also procedure 1-2-3+).

Indicators presented above use only human senses to detect the threat - which is important because do not require any additional cost of purchasing and maintaining new equipment or training its users. Additional value of those indicators is that every person working in a HCC could be a “detector” of CBRN accident after relatively short training.

But unfortunately, human senses have limitations:

- We cannot detect radiation.
- We cannot detect bio agents at all or early enough to prevent contamination.

- We can detect some of chemical agents starting with very high concertation which is already deadly.
- Some chemical agents have no colour or odour and cannot be detected by senses.
- There are substances with pleasant smell which could be dangerous.

This is why use of detection equipment is very often the only way to detect the threat or to detect it early enough to react properly.

11.2. Requirements for detection equipment

In general, two types of CBRN accident could happen:

- Unintentional – which could happen as a result of human error in transportation or be effect of failure nearby facility.
- Intentional – which is criminal or terrorist type of action.

Decision about use of detection equipment should be always a matter of analysis.

Intentional type of attack must be also taken into consideration, CBRN type terrorist attack is often classified as low probability – high impact action. It means that it is not very likely to happen but if it happens number of casualties could be huge.

Some countries are more exposed to terrorist attack than the others. In those more exposed countries like hood of CBRN attack is bigger and stronger response or better preparedness level is needed, including better equipped detection system.

The first strong and very general recommendation is to elevate awareness level among HCC staff and provide dedicated training in detection by senses (indicators of CBRN incident).

Requirements for detection equipment in HCC:

- Simplicity – to shorten training time and assure possibility to use by non-professional users.
- Low purchasing cost – low cost makes possible use of more detection units and do not create big pressure on always limited resources.
- Low maintenance – to not complicate daily use of it and make it always ready for action.
- Wide scope of detection – due to unknown character of agent to be detected.
- Short detection time – to detect the threat as fast as possible.

Please keep in mind that every existing detection equipment could generate false alarms.

There two types of false alarms:

- False positive alarm means that equipment informs user that there is an agent detected (in the air, water - in analysed sample in general) while, in reality, there is no agent present.
- False negative alarms happens when equipment informs user that there is no agent present while in reality there is an agent present.

National/local regulations concerning qualifications of detection and identification of dangerous material staff should be followed/respected (required skills, education level and specialization, trainings needed, required PPE equipment etc.).

11.3. Detection equipment recommendations

The decision on the selection of the appropriate CBRN detection equipment should be preceded by a threat analysis dedicated to the HCC.

Many parameters should be taken into consideration:

- Level of terrorist threat of the country/region.
- Degree of threat attributed to entities or VIP present at the hotel or the degree of threat attributed to the event to be held at the conference centre.
- Level of risk of unintentional release of CBRN material (proximity to chemical plants or warehouses, transport routes for CBRN agents).
- Availability of CBRN materials.
- Potential effects of use.
- Alternative detection methods.
- Cost effective.
- Simplicity.

11.4. Recommendations for chemical hazard detection

Chemical incident is the most likely one out of all CBRN incidents due to large quantities of chemicals used in the industry, easiness to acquire them, transportation of dangerous good (where chemicals are the most widely transported), high toxicity of C agents etc. It means detection system should me mainly oriented on detection of chemicals.

For early detection of chemical incident, we recommend use of:

- Detection papers. They are designed for a battlefield and have limited use in other locations and are useless in chemical industry, storage, transport .
- Detection tubes with electric pump and with spare manual pump.
    - If threat level coming from C or E agents is elevated in particular country or region or a HCC are interested in enhanced level of identification of unknown chemicals (i.e.. high level of false C or E attacks for business disruption) we recommend use of more sophisticated equipment with identifications potential like.
- FTIR Fourier transformed infrared radiation absorption spectral analysis. That technique requires a sample of optical density higher than gasses are characterized with, so if applicable to gases requires special ultra-sensitive equipment.
- Raman spectrometer, based on scattering of electromagnetic radiation induced by LASER. Raman spectrometry is very specific but produced signal is weak and requires amplification.
- Ion mobility detectors developed mainly for military use also applicable in security related services and industries detects characteristic fragments of the compounds of interest, thus they are not universal and depends on the fragmentation component of the detector.

11.5. Recommendations for Bioagents detection system

In order to exclude an event with a biological agent, we recommend the use of rapid detection methods:

1. **Protein detection**

   This method relies on the assumption that a biohazard has a form of a protein and thus is a very rough approximation since many non-hazardous proteins may be

present in the analysed sample. It is however extremely fast, cheap, accurate and sensitive as much as it is non-specific. It is based on Bradford's Blue G-250 attachment reaction to amino acids. The typical kit consists of two reagents-containing tubes

2. **Immunochromatography**

Advantages:

- Simplicity – take the test material with a swab, add the buffer included in the kit, mix, apply in the bowl marked "sample" and read the result; one band in the control line – negative result; two lines (in the control and the test lines) – positive result.
- Execution time – the result within a few/several minutes depending on the kit.

Disadvantage:

- Level of detection is low.
- False negative results.

3. **Bioluminometry**

Main features:

- Could determine the content of adenosine triphosphate (ATP), compound present in every living cell.
- Simplicity – collect the tested material with a swab compatible with the device, place it in the bioluminometer and read the result.
- Very quick determination of the presence of microorganisms in the tested sample – 10/15 seconds.
- Low sensitivity to spores.
- Low costs.

4. **Real-time PCR**

This method is based on amplification of the selected fragments of DNA chain. It undergoes in three steps (i) disintegration of DNA, (ii) prolonging DNA primers and (iii) formation of a new DNA strand. The selected fluorescent dyes are attached to visualize the reaction progress. The PCR method is very sensitive, repetitive and specific. However, sample detection time is about 2 h in the modern instruments. Nowadays it is available as a portable version.

11.6. Recommendations for ionizing radiation detection

Detection of radiation

Gas detectors

Following the rule that any device is better than no device for ionizing radiation detection you may purchase absolutely every available device on the market.

Is important remember that every device for ionizing detection should be calibrated and operated by the trained staff, to avoid error readings or misunderstanding of correct measures.

For radiation detection we recommend two types of detectors:

1. **Personal or portable detectors** (personal dosimeter,).

Dosimeter measures the dose of absorbed radiation. The historical dosimeter measures a total absorbed dose of radiation over time. Such device is thus assigned to a person.

Secent type is direct reading dosimeter which allows the current control of the absorbed dose. Over a specific time period.

Personal Radiation Dosimeters

This type of detectors is sensitive, simple, use to use and fool proof.

Advantage:

- Cheap.
- Could locate source of radiation.

Disadvantage:

- Detects only gamma radiation
- Detects absorbed dose, not a dose rate at a particular time instant

- Ionizing radiation Contamination detector (portable)

Types

There several types differing by methods of signal generation, accuracy, utility features

- Gas detector e.g. Geiger-Mueller Counter

- Scintillation detector
- Semiconductor detector
- Thermoluminescent detector

Advantage:

- Most of contamination detectors are multifunctional devices, for that reason you may switch modes to measure: surface contamination [Bq/cm2], or dose rate [Sv/h].
- The devise is quite cheap and simple in use.

Disadvantage:

- It shows only the external exposure and only from gamma radiation (dose rate mode).

Spectrometers; radiometers (portable)

Advantage:

- Most of portable spectrometers are multifunctional devices. You may switch the mode to measure: dose rate (gamma and neuron radiation) or analyse appropriate isotope that you deal with.

Disadvantage:

- It shows only the external exposure and only from gamma and neutron radiation (dose rate mode). The cost of purchase is very expensive.
- Spectrometers are operated by the personnel after advanced training.

2. Stationary detector at entrance facilities

Stationary radiation monitors

Advantage:

- Very sensitive stationary systems to monitor/control quite large areas. The system can be connected to national radiation monitoring system.

Disadvantage:

- Quite high costs dependent on the needs of the customer.

Please keep in mind that every existing dosimetry detection equipment could generate strange or unexpected alarms. Possible causes are:

- Elevated natural radiation background in place – elevated background may come from usage of some building material groups, where observed increased content of radioisotopes such as sandstones or granites. These natural materials generate Radon – radioactive gas, which comes from natural decay chain such element as Uranium and Thorium.
- Detection of people after medical treatment with using radioisotopes. These people will not cause any danger for living creatures, but dosimetry equipment will “see” these anomalies in natural background.
- Temporary equipment failure – restart of the device is needed.

11.7. Reaction procedures

After prevention and detection, this chapter focus on reaction procedures if HCC faces a CBRN incident. The presented order of procedures is not relevant in terms of the priority of measures to be taken, and priority ones must be chosen depending on the specific case and several procedures must be implemented at the same time.

12. Emergency response

These measures are generic and are suitable for any type of emergency. They are divided into public and staff section

Situation analysis, staff:

1. Stay calm.
2. Try to find out what the source of danger is, collect information and report to HCC security or authority in charge.
3. In the event of an obvious danger, not leaving time for communication with security, make an evacuation decision yourself based on your assessment and knowledge of surroundings.
4. Otherwise, contact HCC security for evacuation directions.
5. Analyse if evacuation routes are safe to move through, check that it is safe to move along the planned route. .
6. Do not expose yourself to immediate danger - protect yourself (use your PPE).
7. If evacuation is not possible, analyse the shelter possibility in a safe room.

Situation analysis, general public:

1. Stay calm.
2. Try to find out what the source of danger is and who is in charge.
3. If possible, contact security, ask for directions.
4. In the absence of professional advice make an evacuation decision yourself.
5. Check if it is safe to move.
6. Do not expose yourself to immediate danger If you have any PPE items like gloves or Face Piece, make use of them.

Evacuation

As an important group in the HCC, the staff responsible for each area play a key role in evacuation. The following are general guidelines for organizing an evacuation in such areas. However, during an evacuation they should follow specific instructions implemented for security manager. Detailed procedures are in "Evacuation" chapter.

Evacuation guidelines:

1. Evacuate the room/area in accordance with the emergency instructions.
2. Consider alternative escape routes in case of possible danger along the main escape routes (including windows). HCC security should announce which evacuation routes are off limits.
3. Minimise the time spent in the danger zone.
4. Maximize your distance from the hazard.
5. Go to the evacuation assembly point indicated by the evacuation leader.
6. Follow the instructions of security at the evacuation assembly point.

Evacuation of VIP

1. VIP security will initiate their evacuation based on their own procedures and on the procedures agreed upon during advance visit or security briefing.
2. HCC should analyse if VIP evacuation impacts the public evacuation, in particular impedes it and take the corrective measures in that case.

Shelter in place

In the case of releasing CBRN agents and lack of ability to evacuate the affected area, try to find shelter to guarantee temporary cover. It is an emergency measure - choose it only as a last resort (2 hours maximum).

For more details go to “shelter in place” in general procedures.

Post evacuation

1. Keep calm.
2. If you feel any effects of the contamination, seek medical attention.
3. If you may have been contaminated, do not hide it from the emergency services - this will allow them to take appropriate action, which may save your life.
4. Follow the security or emergency services instructions arriving on the scene.

13. Procedures

13.1. 1-2-3+

The 1-2-3+ procedure is a tool to assist in the process of recognition and risk assessment during incidents involving CBRN agents. This universal method is used during incidents where the victims exhibit symptoms of unknown origin and the circumstances of the incident are not clear. If two are encountered unconscious or betraying acute ailments of unknown origin, approach with caution. With three or more victims, retreat to a safe location and immediately begin the notification and alarm process.

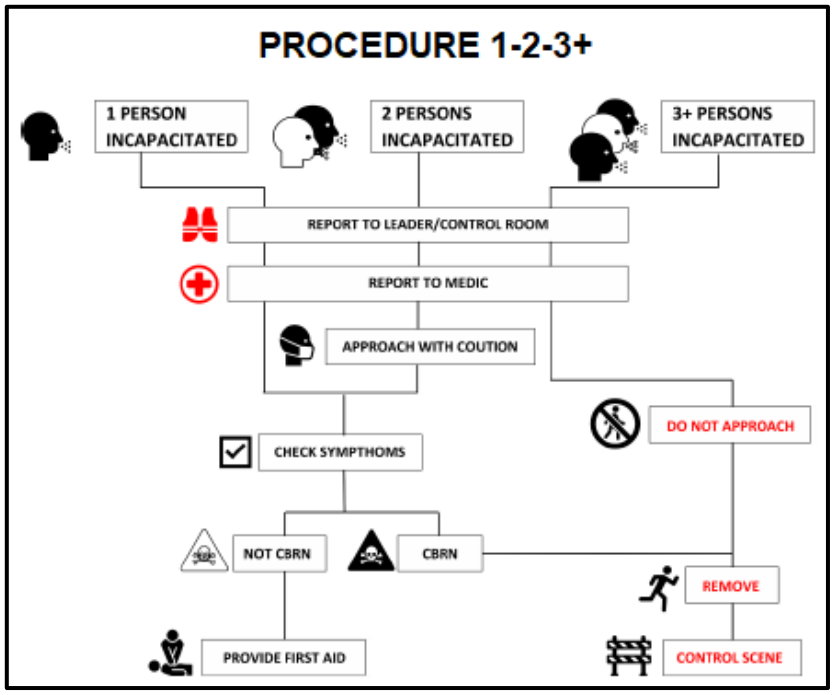

Figure 11 Procedure 1-2-3+

Source: Own source

Follow the steps below:

- One individual complains of symptoms of unknown origin or is unconscious and the external environment within the incident does not indicate a potential threat, the standard mode of action is followed without additional precautions (if the person is conscious there is a possibility to inquire about the causes).
- Two persons injured or unconscious due to unknown causes, proceed with special precautions.
- Three or more persons injured or unconscious due to unknown causes, proceed with extreme caution, retreat and the remaining persons to a safe distance, inform the emergency services, facility security and management.

13.2. METHANE

METHANE is a mnemotechnical protocol for the reporting of mass incidents by emergency services. It provides sufficient information for emergency coordination services to decide on the allocation of appropriate resources.

This protocol can be adapted to the HCC's existing notification and information procedures, in order to more effectively transfer key information to the emergency services. This may ensure that the initial response is appropriate, reduce number of casualties and guarantee the safety of the emergency services called to the scene.

In the case of an incident not falling under a major incident, it is possible to use the ETHANE protocol.

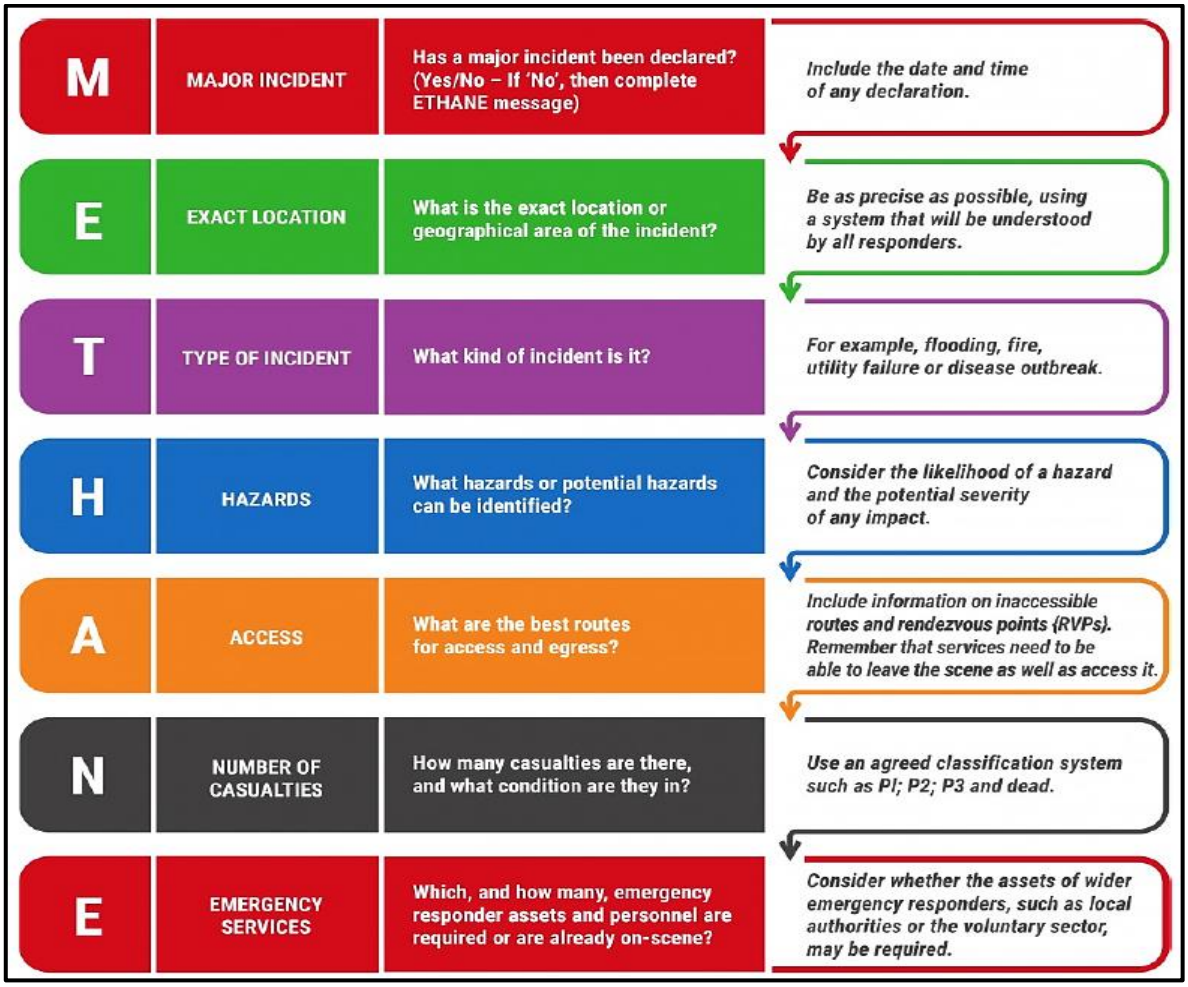

Figure 12 METHANE report

Source: https://www.jesip.org.uk/downloads/m-ethane-full-version/ Access:[05.2024]

13.3. Remove, remove, remove

The general scheme of action when encountering a potentially contaminated person describes a series of actions that should be taken.

Its' main feature is to protect oneself from contamination while assisting the affected person (remotely, without touching or interfering with outer clothing).

Figure 13 Remove, Remove, Remove procedure

Source: https://www.protectuk.police.uk/advice-and-guidance/response/remove-remove-remove-guidance-hazardous-substance-exposure (changed)

In prescriptive form, give information (remove, remove, remove):

1. Remove yourself from the area of exposure agent (liquid, gas exposure, etc.). Preferably go outside the building - be in a fresh air atmosphere. In case of skin injuries, burning, itching or pain, try to redirect the person or provide them with water or other available liquid (try to wash it off and relieve the pain). A report should already be made at this stage – METHANE.
2. Remove outer clothing if contaminated. Avoid pulling clothes over your head (if possible), try to keep hand contact as small as possible with clothing. Do not eat, drink or scratch. Do not remove clothing stuck to the skin.
3. Remove the substance from the skin is affected. Rinse continually with water if the skin is itchy or painful. If the substance in not painful or itchy, use dry, absorbent material to either soak it up or brush it off.

If you do not need help, and you are safe, find out if other people do. With extreme caution, inform the relevant services, remotely give instructions in accordance with the above procedure.

14. Evacuation/rescue pack for VIP

Evacuation of people after CBRNe attack or accident is one of the most important procedure among all the procedures provided in this report.

Proper evacuation leads to shortening exposure time and reduce number of exposed people which means lower number of fatal casualties, less severe injuries, lower dispersion of the agent, etc.

Evacuation after CBRNe accident differ from other types of evacuation. Effects of attack could not be visible thus improper route of evacuation is more possible than in other ones (like during fire) which could make situation significantly worse. This is way it is very important to understand evacuation principles, organization, responsibilities, phases and to exercise it cyclically.

In most venues there is already evacuation plan, it should be updated with information and action specific to CBRNe attack or incident instead of creation of new evacuation plan dedicated only to CBRNe. This approach creates perception that CBRNe incidents are one of possible threats we have to take into consideration. Creation of new security documents (informing plan, evacuation plan, training plans) could lead to neglecting them if no such incidents happens. Because of complexity of the procedure and its importance evacuation plan should be carefully prepared and checked periodically for its applicability and effectiveness. This evacuation plan has to be discussed with VIP security prior to their arrival to the venue. VIP security have their own procedures for evacuation and, probably, for CBRN related evacuation too. These procedures may conflict with HCC ones, and it is the joint task of both services to agree them. In particular, a situation when VIP security procedures compromise public safety during CBRN incident should be avoided.

Crisis communication details between HCC and VIP Security including participants of the information loop should be agreed upon.

Points of intersection of decision loops of HCC security and VIP Security should also be agreed upon.

The measures listed are generic and must be applied to VIP with the necessary adaptations.

14.1. Evacuation principles

Evacuation is a process of elimination of exposure to the threat/risk to the people be removing them from dangerous location.

Successful evacuation should be:

1. Fast – the shorter exposure to the threat (in this case to CBRN agent) the lower risk of contamination or poisoning and less severe effects of contamination.
2. Complete – all the people should be evacuate or all the people needed instant evacuation (see shelter in place).
3. Safe – organization of evacuation should be safe to the visitors and workers, which includes safe routes of evacuation (extremely important for CBRN evacuation), use of dedicated equipment including PPE.
4. Managed – people responsible for evacuation have to know what to do at every stage since announcement to arrival to the dedicated rescue services (firefighters, Police, etc.), including management of the people at assembly points.

14.2. Evacuation plan

The evacuation plan is designed to prepare information for staff to evacuate the building as quickly and safely as possible. In order to ensure that staff members are sufficiently prepared, these plans must cover all relevant scenarios of possible crisis situations. Emergency situations can include everything from natural disasters, industrial accidents, transport accidents, terrorist attacks, structural failures, or fires.

What should an evacuation plan contain?

Define the roles and responsibilities of functional staff. When an incident occurs, the people involved will expect clear instructions from the services leaders on exactly what to do in the situation. Create a clear chain of command including who has the authority to decide, coordinate and lead an evacuation in the HCC as well as specific areas.

Steps for developing an evacuation plan:

1. Develop various options for dealing with different hazard

In order to develop an effective evacuation plan, start with some basic questions to develop a pattern of responses to the primary and extraordinary hazards that your facilities may face.

Develop an event tree for different extreme scenarios analyse it what, after defining risks levels, allows you to create an emergency plan. This exercise also helps to raise any security and safety incident preparations to the level of collective awareness in your working environment.

2. Identify schemes of action in each zone

Make floor plans or diagrams of the premises and then inform all functional staff so that they know their evacuation routes. Best practice also requires the development of a separate evacuation plan for people with disabilities. A good evacuation plan will also include primary and alternative escape routes. Establish a decision and information loops implementing the alternative escape routes.

Mark all escape routes, fire exits, and special places (first aid kits, escape bags) with clear signs. Describe in detail the tasks and roles of the functional staff in their zones with a detailed division of all evacuation phases in the zone.

Designate a safe assembly point for dedicated zones taking into account hazard options (e.g. CBRN).

Finally, confirm that evacuation routes and assembly points can accommodate the expected number of evacuees. Each plan should be unique to the individual zones, and floors to which it is dedicated.

Develop a plan for the organization of the evacuation assembly point, and designate the location, equipment, and person responsible for the medical assistance and initial decontamination station.

3. Create a communication plan

During the development of the plan and evacuation drills, establish a main and backup communication plan for internal and external use, and define the available means of communication, radio communication channels or telephone numbers.

This communication plan must clearly define the circuits and flow of communication, so that anyone on the HCC staff knows who to pass information on to, from the bottom up to the person responsible for the security of the facilities.

You should also appoint a liaison officer whose main responsibility is maintaining contact with the fire and emergency services and disseminating information to key stakeholders, including employees and customers, in the event of a loss of communications. If necessary, assess whether your crisis communication plan should also include contacts with the local community, suppliers, transport partners, and government officials.

The ability to send notifications via email, phone, text messaging, and the mobile app provides the opportunity to reach everyone in the building using preferred and secondary communication methods - allowing the widest possible distribution of messages. It also allows the fire and emergency services to reach the site as quickly as possible.

In the case of post-threat response, the communications team will need to communicate to relevant stakeholders how the situation affects the company, what actions they should take, and what the next steps are.

4. Check your tools

Create a schedule to confirm that emergency equipment is up to date and functional, including:

- Megaphones.
- Fire extinguishers.
- Means of communication.
- First aid kit equipment.
- Escape bag equipment.
- Recharging the batteries of torches, radios.
- Periodic check of other alarm equipment.

5. Practice the evacuation procedures

The evacuation plan should include a detailed guide as to when for whom and in what form to conduct the drill.

Running regular evacuation drills minimizes any confusion and helps to observe how the various evacuation steps should work and ultimately reduce the risk of panic in the event of a real emergency.

Hazards spread rapidly and often second can be decisive - so it is essential to prepare and train at designated positions at an individual level before a potential evacuation.

Key figures for the evacuation process should meet quarterly and should plan annual or half-yearly training at different levels of operation for different incident scenarios.

Coordinate the evacuation plan in advance with the police, emergency services, local authorities, and neighbours. Be sure that staff with specific responsibilities are trained and that all staff has had their training drills. Also, remember to inform the police of the action taken during any incident.

14.3. Phases of evacuation

Evacuation is a quite complex action, it consists of three phases:

1. **Planning and decision making phase.**
2. **Managing evacuation.**
3. **Activities at the assembly points, well-being of evacuees, triage, medical care, provisional decon.**
4. **Assembly points management.**

First phase is about preparation to the incident including creation of evacuation plans, preparation of assembly points and equipment needed, provision of training to the people involved in the evacuation process. In some cases, especially if the CBRN agent release is sudden on evacuation route, it is better to stay at the place and wait for help. This decision is not easy and obvious and several factor should be taken into account this is why should be considered prior an incident. As preparation to the incident is a constant process it could be said that this phase is ongoing and ends with evacuation announcement.

Second phase describes management of the evacuation process and actions to be taken during different stages of evacuation. This phase, due to it's complexity is divided int three stages:

- The first stage is related to the movement of people from the rooms/spaces towards the exits to the evacuation routes.
- The second stage is related to the movement of people along the escape routes to the emergency exits of the building.
- The third stage is the exit to the outside of the building and the movement of people to the assembly point or outside the premises.

Third phase of evacuation is focused of management of the people at assembly points till the arrival of rescue services.

Evacuation – Phase 1

Conditions for ordering evacuation in CBRNe events:

- Information about a suspected terrorist act (e.g.: planting an explosive device or a dangerous agent dispenser).
- An event posing a threat to the health or life of the persons present (e.g.: emission of toxic or substances, presence of explosives or explosive devices).
- Fire alarm or fire leading to the release of toxic substances or heavy smoke.
- Inform VIP security, implement the agreed plan for VIP evacuation

Evacuation or shelter in place - decision making process

In regions where there are industrial plants using hazardous substances in the production process or located close to the roads and rail infrastructure used for the transport of dangerous goods, a decision-making system for preventing and responding to violent incidents is needed.

It is necessary to establish internal evacuation mechanisms/procedures, taking into account the technical infrastructure (ventilation system, fire barriers, other technical infrastructure), the adjacent area and the prior development of potential incident scenarios.

The evacuation plan plays a key role in safety management, at the time of the emergency and during the implementation of the evacuation process. In case of VIP presence, the evacuation plan has to be agreed with VIP security.

In order to develop effective evacuation strategies outside buildings, weather conditions, the direction of the spread of contamination should be assessed first and foremost. The organisation of operations inside the facility should focus on estimating the optimisation (orientation) of evacuation routes, as far away from the incident as possible, in a safe direction.

Successful evacuation allows people to be removed from the affected area and avoids their exposure to harmful concentrations of hazardous substances.

An inappropriate evacuation decision can have negative consequences if people are moved into a contaminated area or an area where the contamination enters (e.g. according to the direction of the wind).

Evacuation of VIPs is usually governed by the internal procedures of their security staff. It is essential to agree the basic principle of VIP evacuation, possibility of VIP decontamination, medical treatment etc.

Sheltering in place may prove to be a worse option than evacuation if shelters are leaking /improperly prepared, people are not informed of their presence, there is a lack of information on when they are to leave shelter or the exposure to toxic substances lasts for a long time.

Decision-making process on a selective evacuation plan in the event of an incident inside a building without the possibility of evacuation by alternative routes should take into account the following parameters:

- Remaining time to contact with contamination.
- Distance from incident site.

Similar assumptions can be made for the occurrence of an incident outside the facility with the option of sheltering in place in the building. This procedure in not considered for VIP as there will always be attempt to evacuate them outside the endangered zone. That require assuring presence of required evacuation PPE offering best protection.

The decision support matrix therefore provides for two types of response:

- Evacuation (please keep in mind that if threat is coming from outside evacuation could be directed towards inside of HCC - it is called invacuation).
- Shelter in place.(Not for VIP)

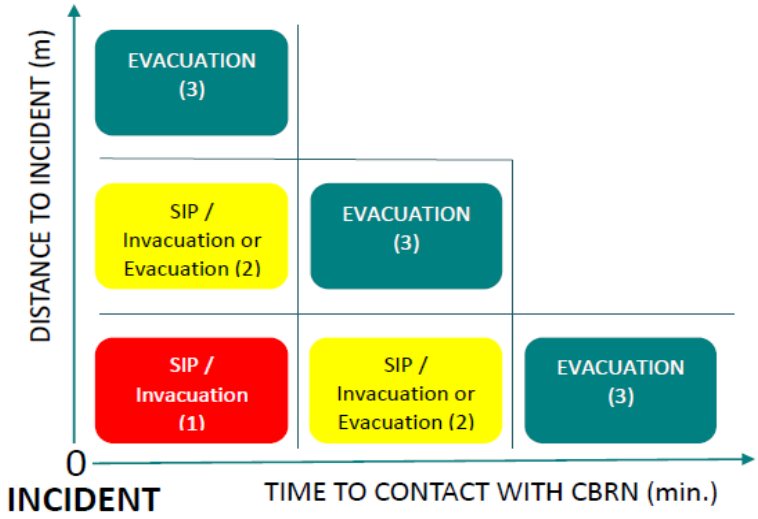

Figure 14 The diagram of decision making depending on distance from the threat and time available

Source: CBRN Mall Project

The X-axis was defined as a time parameter, depicting the spread times of hazardous agent in the facility. The Y-axis was divided into distances from the incident site.

In order for the decision-making process to be effective, it is also important to assess the rate of diffusion of hazardous gases in an enclosed space. The further away we are and the more time we have before the contamination reaches us, the more effectively we can safely evacuate people out of the affected facility. Considering SIP, a volume of a shelter has to be taken into consideration as falling oxygen and building-up carbon dioxide concentrations may lead to irreversible health damage or death.

<u>This decision-making matrix can be used when:</u>

1. Shelter in place. Diffusion time for hazardous materials is rapid and evacuation time insufficient.
2. Shelter in place or evacuate. The diffusion of hazardous materials is not very fast (evacuation time is sufficient), the distance to the hazard is also sufficient for evacuation. In this case, other factors such as people with disabilities, young children, problem with the capacity of emergency exits may influence the decision to shelter in place.
3. Evacuation (or invacuation) depending on the location of the contamination source – inside or outside). Evacuation is possible because the distance to the incident and the time needed to evacuate people outside the facility is sufficient or the speed of spread of the contamination is not high.

The evacuation decision must include:

- Information on its coverage.
- Information on how and in what order to leave the area.
- Identification of evacuation routes and areas designated for evacuees.

Preparation for evacuation

In the case of situations involving a suspicious, unidentified object and an expected evacuation announcement, the staff involved in the evacuation process should be initially informed of the situation. This uses code words such as: "CODE 101", given by internal communication system.

Pre-evacuation actions:

1. Collect the necessary equipment to guide the evacuation (e.g.: reflective vests, means of communication, torches, PPE).
2. Check evacuation routes for safety in particular:
   - Choking points - corridors, passageways or exits.
   - Rubbish bins, flower pots.
   - Permeability of escape routes.
   - Permeability of emergency exits.
3. Check the designated assembly points.
4. Prepare equipment to organize assembly points (e.g.: medical bag, thermal blankets, water, megaphone for crowd control, initial decontamination kits).
5. If possible, check fire roads or access routes for public services.
6. Take up positions and directions in assigned areas according to the evacuation plan.
7. Keep people out of the danger area.
8. Inform VIP security staff

Evacuation announcement

If the facilities have any kind of Voice Alarm System (VAS), the system should be used for transmission of the evacuation announcement. The message should be preceded by a special signal to draw the attention of the listeners or a verbal announcement "PLEASE ATTENTION!" with a gap of 4 seconds between the announcement and the message.

Announcement or warning signal and the message should be broadcast sequentially until changed in accordance with the evacuation procedure or manually muted.

The system used, should provide the possibility of automatic broadcasting of emergency signals in the event of the detection of a hazard or its occurrence.

Independently of the automatic activation of the system, it should be possible to broadcast "live" messages using a microphone in the reception or security room. This system should have priority over other public address equipment and should ensure that hazard messages are also broadcast in foreign languages (e.g. English).

Method of evacuation announcement

The evacuation announcement message should include:

- Information on the decision made as to the type of evacuation (shelter, shelter or evacuation, evacuation).
- Identification of directions for safe passage to assembly points.
- Dangerous parties/directions/entries.
- Prohibition of the use of specific facilities.

Agree the methods of notifying VIP security about incoming threat

If the decision is made to evacuate, an announcement should be made, an example of the following:

"ATTENTION, ATTENTION, ATTENTION! THREAT HAS BEEN DETECTED AT THE FACILITY. PLEASE PROCEED TO THE NEAREST EMERGENCY EXIT. AVOID ANY CLOUDS, SMOKES OR AREAS WITH UNUSUAL ODOURS. PLEASE REMAIN CALM IN YOUR DESIGNATED EVACUATION AREAS".

Evacuation - Phase 2

Phase 2 consists of three stages:

- Stage one - Evacuation from premises.
- Stage two - Evacuation by emergency routes.
- Stage three - Moving to assembly points.

Plan during pre-visit preparations the way VIPs are evacuated by their staff

STAGE ONE - Evacuation from premises

As indicated in the figure below in a sudden terrorist incident with CBRN agents, evacuation is carried out in a directional manner (i.e. from the site of contamination, via evacuation routes, to emergency exits, and then on to designated post-evacuation assembly points or off-site).

Figure 15 Example of evacuation route in case of CBRN attack

Source: Own source

General advice to staff and administration:

1. Upon hearing the evacuation signal, stop work, make sure that all persons in adjacent rooms have heard the evacuation announcement.
2. Keep calm.
3. Take your mobile phone but leave other belongings behind.
4. Assess the situation (decide whether you can evacuate and whether you will have time to evacuate staff and customers) - see decision-making matrix.
5. If you do not have time to escape from the spreading hazard - see shelter-in-place procedure.
6. If you have a disabled or injured person report the situation to the evacuation coordinator or the functional staff in charge of the area you are in and ask for help.
7. If you are not in contact with security, designate a person or persons to assist with injured or disabled persons - take the initiative.
8. Always evacuate in the opposite direction to the danger - indicate to people the direction in which they should evacuate.

9. If you are isolated from an exit on the ground floor of the building try to evacuate through a window (if you can do it safely).
10. Try to be the last to leave the premises.
11. Lock your doors when you leave the workplace, this will limit the spread of contamination - do not lock them.
12. Do not return under any excuse, even if you see people who need help but are in the contaminated area.
13. Walk, do not run to the nearest exit or staircase, if you have comfortable walking shoes, use them, you may not know how far you will be evacuated from the building.
14. Inform the coordinator when the evacuation of your area of responsibility is complete.

STAGE TWO - Evacuation by emergency routes

General instructions:

1. The building at risk must be evacuated using suitably marked escape routes, these routes are generally corridors and staircases used for normal day-to-day pedestrian communication.
2. Do not use passenger or freight lifts, service walkways, ducts, installation platforms, or other similar technical systems and equipment for evacuation purposes.
3. When walking in corridors, on stairs, or ramps, the following rules must be respected during an evacuation:
   - Remain calm and quiet.
   - Do not run or overtake others.
   - Do not push people ahead of you.
   - Do not stop or turn around unintentionally.

Functional staff Person in charge of specific zone

1. Get an overview of the general situation and the situation in your area.
2. If you can, use the necessary equipment available.
3. Direct people to the closest emergency exits, in the opposite direction to the danger.
4. Prevent panic among people in your area.
5. Call for calm, informing about evacuation directions.
6. Take care of those who need help (not only the injured but also people with special needs).

7. Before entering the stairwells, check the stairwell by the exit door for signs of contamination (e.g.: smoke, fumes, or unconscious persons).
8. Do not allow anyone to bring large items of luggage into the stairwell or make telephone calls.
9. Keep contact with the evacuation coordinator during the evacuation, report any problems in your area.
10. At the end of the evacuation, verify that all rooms in your area (floor, car park, corridor) have been evacuated.
11. Report in detail to the evacuation coordinator about the situation.

Coordinator

1. Once the evacuation procedure has started, transmit to all areas the decision on the assembly points after the evacuation or any other decision taken.
2. Inform the services about the situation, if possible, provide safe directions or safe points for picking up the emergency services.
3. Send functional staff and persons involved in the evacuation process to the indicated directions according to the evacuation plan.
4. Close fire zones to reduce the spread of contamination.
5. Shut down all air-conditioning and ventilation systems and other systems or objects that circulate air and open the smoke dampers (in the event of an internal emergency).
6. Monitor the situation through available video surveillance, if unable to stay, go to a safe place outside the facility.
7. Maintain constant communication with the zones and ask for situation reports.
8. Keep constant communication with the emergency response team.
9. Once the evacuation is complete, report the situation in the evacuated facility to the emergency response team or facility director/administrator.

STAGE THREE - Moving to assembly points

Criteria for the selection of the evacuation assembly area.

It is recommended that the following criteria should be used in the selection of the evacuation assembly area:

1. The area should be known and easily accessible to people who are evacuated from the building.
2. This area should be downwind of the site of the CBRN agent release.

3. Due to the different possible wind directions, at least two evacuation areas should be prepared in the plan and a choice made with wind direction data.
4. Should be capable of housing all evacuees from the facility.
5. Should be far enough away to avoid falling debris, glass fragments, collapsing structures, and the spread of a hazardous event - the distance from the building should be at least equal to the height of the building.
6. The location of the assembly points should be determined in a way that does not interfere with firefighting and emergency response operations by the specialized services.
7. Designate alternative evacuation assembly points in the event of a displacement hazard (contamination cloud).
8. If the evacuation assembly point is on the other side of the road, designate an authorized person to control traffic on the road to keep people crossing the road safe.
9. Coordinate evacuation assembly points (especially in a crowded urban area) with neighbouring facilities to eliminate overlapping of the same emergency sites.

Evacuation – Phase 3

Organization of the evacuation assembly point

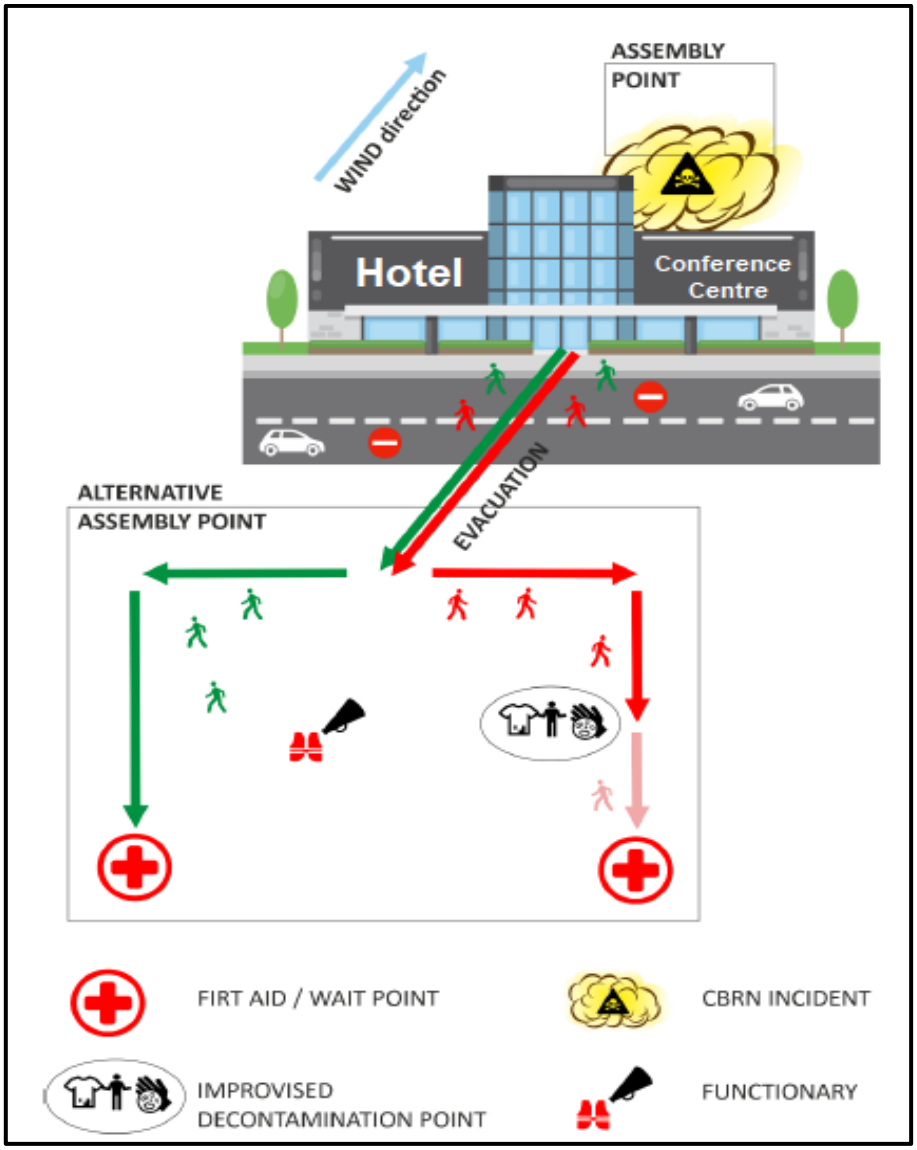

Figure 16 Organisation of the assembly point in case of CBRN attack

Source: Own source (adapted from CBRN Mall Project)

1. Assembly points should be indicated by the director/administrator based on pre-selected alternative and main assembly points.
2. The location of the site must guarantee full safety for evacuees, regardless of the danger spreading.
3. The functionary who is responsible for organizing the evacuation assembly point should take charge of crowd control and preselect people entering the assembly area.

4. In addition, persons should be designated at the point to:

- The organization of a pre-medical aid post.
- The organization of improvised decontamination points up to the arrival of the services.
- The organization of traffic - blocking the assembly point against the entry of any vehicles.
- The organization of possible support points - equipped with water, and thermal blankets.
- Reducing contamination spread (keeping removed clothes in one place, collection of used decon material – tissues, water etc.).
- Collection of valuable but possibly contaminated belongings.
- Registration of people for further investigation (medical, epidemiological, crime).

Evacuation of VIP: VIP are evacuated by their security. The role of local staff is to facilitate their evacuation. The tasks may include:

1. Providing any information that may facilitate the evacuation.
2. Show the escape route or alternate one, inform about the hazards.
3. Assist in clearing the escape route.
4. Assist in providing safety of operation at large.
5. Facilitate initial decontamination if necessary.

15. Shelter in place

Shelter in place is a procedure that can be adopted when safe evacuation cannot be carried out. In the case of the release of CBRN agent and the inability to evacuate the affected area (cut off exits, escape routes), try to find shelter to provide temporary shelter. This is an emergency measure and should be an option only as a last resort and used up to a maximum of 2 hours.

In the case of VIP visits, the HCC must have defined the possible places for shelter in place, and it is then up to the VIP's personal security services to decide whether or not to use them, depending on the specific case.

When choosing a shelter, try to:

- Keep calm.
- Assess your condition.
- Turn off the ventilation.
- Seal all window door openings (e.g. with tape) or place damp towels at the bottom of the door to limit air leakage under the door.
- Make sure the space you are in is safe - are you far enough away from the contamination, have you sealed/protected the room from volatile substances/gas /if you think not then look for a safer place.
- Contact security, inform them of your location and the number and condition of the people gathered.
- Analyse whether you may have come into contact with a poisonous substance, check your clothes for traces of the unknown substance (if so, see procedure for improvised decontamination).
- Check for skin injuries/irritations, tearing, wounds.
- Never eat, drink or smoke in shelter and avoid hand to face contact to minimize the possibility of accidental exposure to CBRN agents,
- Estimate how much air you have enough for.

16. Initial decontamination

Decontamination is the physical, chemical or disinfection process of removing a contaminant (e.g.: harmful chemicals, micro-organisms or radioactive materials) from body surfaces, objects or facilities.

Due to the complexity of the problem, decontamination should be carried out by specialized emergency teams. However, initial decontamination must be carried out to minimize the duration of human exposure to the hazardous substance, minimizing the effects of the hazardous substance on the human body.

When and where should be defined by the HCC security officer, as it will vary according to the specific facility.

Improvised dry decontamination

Unless the victims have signs or symptoms of exposure to corrosive or irritant substances (for example, redness, itching and burning of the eyes or skin), should be carried out on exposed skin surfaces.

As a first step, the hazardous substances should be removed (or adsorbed) from the skin surface with any available dry adsorbent material, such as paper tissue, nappies, sponges, sanitary pads, clean cloth, etc., avoid rubbing the substance into clothing and skin (this may cause the substance to be absorbed into organism through penetrating deeper into the skin or clothing).

All waste resulting from decontamination should be left (if possible, in bags) for later decontamination at a later stage (in one place or in dedicated places) out of evacuation route.

Pre-decontamination (dry) using gloves, sponges, and towels with cleaning or deactivating substances included in the pre-decontamination packs should be an option, especially if the contamination is a non-caustic liquid or water-reactive chemical.

Agree with VIP security their procedures regarding provisional dry decontamination and if/how to conduct it at HCC

Wet decontamination

Should be carried out if the contaminant is corrosive or is in particulate form). Depending on the nature and degree of the contamination, wet decontamination (water or soapy water, top to bottom) may be necessary. Whether wet decontamination comes after dry decontamination should be the subject of a dynamic risk assessment by emergency services personnel at the scene. However, the critical steps of rapid evacuation, clothing removal, and

dry decontamination should NOT be replaced or delayed when temporary wet decontamination is established.

Improvised wet decontamination (using water)

Should only be used if the signs and symptoms of the affected persons are consistent with the exposure characteristics of corrosive substances such as acids or bases, or the contamination has been identified as biological or radiological. Wet decontamination can be carried out using any available water source such as taps, showers, hydrants, sprinklers, etc. Any fluid like drinking water, tea, soft drinks may be used to flush visible contamination from the skin. Such procedure should be carried out outside the evacuation route.

When using this method, it is important to limit decontamination time to 45-90 seconds, and preferably use a cleaning agent such as a cloth or sponge.

Improvised decontamination should not involve overly aggressive methods of removing contamination, as this could lead to the introduction of hazardous substances into deeper layers of the skin.

Agree with VIP security their procedures regarding provisional wet decontamination and if/how to conduct it at HCC

If you possess dedicated equipment for initial decontamination (initial decontamination set) you can use it if you suspect or are sure that a potentially hazardous substance may have contaminated your clothing. Typically those sets have manual but in general required steps are as follows::

1. Evacuate yourself from the danger zone.
2. Inform safety management personnel, if possible.
3. Wear disposable gloves.
4. Remove and unfold the plastic bag for trash.
5. Climb onto the bag and remove any clothing contaminated with the hazardous substance. Do this very carefully so that you do not touch your body with the contaminated clothing.
6. Put on your previously removed watch and jewellery, consider whether sensitive equipment and documents can be decontaminated (e.g. phone, keys, ID card, for example). If so, allow victims to keep these items after decontamination.
7. Remove a pair of gloves very carefully and put them in the bag.
8. Close the bag and put it into a second bag and close it.

9. Wash hands very thoroughly with detergent or soap, rinse hands for 1,5 minutes with water.
10. Do not eat, drink or smoke.
11. If you have soiled other parts of your body with a hazardous substance, try to wash them under running water, using detergent or soap, and then wash your hands very thoroughly by rinsing them with water for 1 minute.
12. While doing the above, take special care not to come into physical contact with other persons.
13. Regularly self-assess your own health, observe exposed parts of your body for redness, swelling, rashes, itching, check for breathing difficulties, dizziness, nausea.
14. Try to remain calm and rational - many people report symptoms of poisoning after such an incident even though they have not been exposed to hazardous substances.
15. Seek immediate specialist medical attention from the services on the scene.

If you have an initial decontamination package follow the instructions below:

Figure 17 Graphic instruction for initial decontamination

Source: CBRN Mall Project

17. Cleaning surfaces procedures

One of the ways dangerous pathogens are transmitted is through contact with contaminated surfaces, where they can survive in the form of spores for several months. Before the arrival of a VIP or the organization of an event with a VIP, HCC must take care, through their cleaning teams, to carry out a more rigorous cleaning of the spaces to be used.

Evidence that indicates possible contamination

These services must also be able to recognize some of the signs indicated as signs of possible contamination, opting, if necessary, to work with trained cleaning staff who carry available and appropriate equipment, chemicals and personal protective equipment. In these cases, special attention must be paid to all surfaces that come into contact with hands, whether in public or administrative areas, examples of the most sensitive areas are the stair handrails, door handles and elevator switches.

The following guidelines can be implemented as a standard, however, to validate the procedures to be used, depending on the type of contamination, the health services of the country should be contacted.

All cleaning staff should be informed and trained about the hazards and the procedures in place. Cleaning of areas not contaminated should be carried out in a standard manner.

The number of cleaning staff should be appropriate to the ability to clean contaminated surfaces efficiently in the shortest possible time.

The cleaning team should only include exclusive and specific personnel for this task, not including employees with other responsibilities (reception, restaurants and bars, etc.).

To clean a possibly contaminated site, these teams must use appropriate PPE, namely:

- Disposable gloves to protect against chemical and biological hazards of appropriate resistance class in accordance with safety standards.
- Safety goggles or safety glasses.
- Disposable chemical and biological hazards protective suit of appropriate resistance class complying with safety standards.
- Disposable protective mask or masks/face pieces of FFP-2 class or filter elements of P-2 minimum.

Recommended management of spilled body fluids:

1. Remove people from the immediate area.
2. Place a "caution cleaning" warning sign.
3. Put on necessary PPE.
4. Cover body fluids and organic parts with disposable paper towels to absorb excess fluids collect and place in a double bag.
5. Cover remaining fluids with disinfectant spray and leave for 5 min.
6. Wipe the area with disposable towels and collect them in a double bag.
7. Wash the surfaces with detergent and hot water using disposable tools and dry thoroughly.
8. Place personal protective equipment in a double bag - secure bags with adhesive tape.

If there is a risk of secondary infection of cleaning service members, quarantine the exposed persons in accordance with the recommendations of the competent services.

Attention: You can find more information about cleaning procedures from guideline developed within project HOTHREAT- “Protection guideline for cleaning services”.

18. Vulnerable points response procedures

This chapter presents guidelines for response procedures to deal with the most common threats that can affect the normal functioning of HCC. As it is impossible to present all threats and scenarios in an exhaustive manner, the procedures indicated are merely guidelines and must be combined with all others mentioned in this report.

18.1. CBRN bomb planting information

General description

One of the most common disruptions to the day-to-day operation is information with threatening information about a possible terrorist attack. These are mainly information provided via e-mail, text message, telephone or sent by mail.

Motives are most often:

- Criminal activities desired to obstruct the place's activity.
- Financial extortion.
- Prank calls.
- Criminal and terrorist activities checking existing response procedures.
- Other criminal and terrorist activities.

The vast majority of these are false alarms often leading to the evacuation of the facilities.

Response to the threat

The person receiving a call/information that a dangerous device has been planted or that an attack is about to take place has a responsibility to:

1. Take the information seriously and as a priority.
2. Obtain as much information as possible from the caller/sender to obtain as much information as possible about the location, size, time of detonation, CBRN agent used, effects it may have.
3. Take notes of the words or text using literally the same wording as the caller/sender.
4. Pay attention to the caller's background sounds and voice to be able to recognize the location from which the call is coming and the caller themselves.
5. Immediately inform those responsible for making key security decisions in accordance

with the security grid specified in the security manuals for the site concerned.

6. Inform the relevant law enforcement services according to the security grid of the country concerned.

The person in charge of security, when receiving a report of an explosive device, immediately follow the recommended course of action.

General scheme of action

1. Stay calm, the vast majority of calls are false.
2. Inform the management of the HCC.
3. Inform VIPs or those responsible for their security.
4. Immediately inform the nearest police station on duty or the relevant CBRN emergency service via the emergency number.
5. Inform the HCC's line security staff.
6. Inform those present of the situation (by app, telephone, or other means of communication).
7. Decide whether to search, not to search, or to evacuate the place, according to the threat level, in accordance with the "search methodology" and considering the national terrorist threat of the country concerned.
8. Instruct CCTV staff to scan the areas under CCTV surveillance to identify a suspicious object/person.
9. If you have ordered a search, supervise it in terms of:
   - The presence of suspicious objects or changes in the environment.
   - Checking front desk, arcades, evacuation corridors, evacuation assembly points, catering areas, toilets, the roof, the delivery area, technical areas.
   - Draw the staff's attention to any unusual behaviour of people present on site or surroundings.

18.2. Bomb threat (dirty bomb)

General description

The ability to obtain the components and the knowledge required to construct a nuclear weapon makes the use of such a means of mass destruction one of the least likely scenarios. Nevertheless, gathering radioactive materials and using them to create an explosive charge is

not impossible. Knowledge of security and how to use radioactive material to construct a so-called 'dirty bomb' still poses a great challenge to terrorist organizations.

A dirty bomb is nothing more than a combination of conventional explosives with radioactive materials. Stuffing a dirty bomb with chemicals is also possible. Among other things, the explosive in this arrangement provides a means of dispersing a dangerous agent.

From the point of view of the possible dangers, the radioactive material itself does not pose an immediate threat to life. The detonation of the explosives and its accompanying effects are much more harmful. The more widely radioactive material is dispersed by the explosion, the less of a threat it poses but recovery after the bigger dispersion could be more challenging.

Using chemicals as a CBRN load in a dirty bomb leads to a dispersion covering a larger area than when using other means of chemical dispersion, and coverage is, at least initially, independent of air movement. The use of these modes of agent dispersion mainly a mass media impact and leads to the creation of intimidation and panic, local contamination, or the massive costs associated with decontamination and the temporary shutdown of the facility.

Only materials with a high level of radioactivity can cause immediate symptoms that may indicate the use of this source of danger. These include:

- A local burn with no known cause.
- Abnormal blood counts, nausea, and vomiting in a group of people, which can occur after several hours to several days.

Similar effects are accompanied by hidden sources of radiation. These are radioactive materials placed in the locations of potential victims (random or targeted at specific individuals). Such materials can simulate and take the form of any object.

The only effective method of detecting the use of such agents is through radiation detectors.

Response to the hazard

In the case of an incident or when radiation is detected by a dedicated device, follow the procedure:

1. Retreat to a safe distance. Identify the air movement direction if possible
2. Protect your respiratory tract from the possibility of dust entering your lungs.
3. Remove outer clothing. Avoid pulling clothing over the head (if possible), try to keep hand contact with clothing as limited as possible, and wash your whole body with water to rinse off dust residues after the explosion.
4. Do not remove clothing stuck to the skin.
5. Move away from the area of influence of the hazardous substance (liquid, gas effects, etc.). In the event of skin injuries, burning, itching, or pain, try to divert the person or

provide them with water (try to wash it off and relieve the pain).

6. Do not eat, drink, smoke or scratch.
7. Remove substances from the skin using dry or water-soaked adsorbent materials (including handy ones such as paper towels, towels, and other clean clothes, e.g.). Take special care not to rub the substance into the skin.
8. Try to keep all contaminated clothes in one place. Collect all materials and liquids used for decontamination in a container and give it to dedicated services only. Those materials still could contain radioactive material and be a source of secondary contamination.
9. Provide emergency medical services/accident coordinator with your name, address for further analysis.
10. Check with radiation detector effectiveness of radioactive material removal or decontamination by specialised service.
11. Monitor yourself if you experience dangerous symptoms immediately call emergency medical services and wait for help.

18.3. Left item

General description

The categorization of left luggage/objects as potentially dangerous (suspicious) is based on an analysis of three elements: the location of the object, the time, and the circumstances of detection.

- Location - not all items left unattended are likely to be suspected. Everything that is hidden, obviously suspicious, and unusual should be considered suspicious. Usually, items left in visible places such as benches, restaurants, toilets, or vending machines are simply forgotten or discarded, however, they also should not be neglected.
- Time - peak hours, highest traffic intensity indicate intentional leaving of an item more than in the morning hours.
- Circumstances - the domestic situation in the country, a state of heightened alert announced in the media, information coming from your own or other business networks about the possibility of an attack, the intensity of attacks in recent times, important of persons or events in the place (VIP) may indicate an increased risk of attack.

The most important factor affecting security is to spot/locate left luggage/objects as quickly

as possible. Awareness training of HCC staff and customers is extremely important throughout the entire process.

If at any stage, you identify characteristics of a suspicious item - follow the other security procedures.

Response to the threat

Rely on 4C's rule:

1. Confirm.
2. Cordon.
3. Call.
4. Control.

Confirm – hazard identification:

1. Go to the area of the object spotted as soon as possible.
2. Ask people in the immediate vicinity if it is their item/baggage or if they have any information as to who it belongs to.
3. At the same time, confirm whether it is possible to identify the owner through CCTV, also analysing their appearance and behaviour.
4. Characteristics indicative of a dangerous item include:
   - Protruding electrical wires.
   - Power sources or electronic components connected to other equipment.
   - Clocks and other time devices combined with any other object.
   - Antennas, mobile phones, radios combined with other items.
   - Objects of military origin (weapons, cartridges, bullets, explosives, etc.).
   - Emitted sounds (ticking, hissing, etc.).
   - Fumes, strange smells, smoke.
   - Strange, nervous behaviour of the object's owner resulting from the observation of the monitoring and witnesses (nervous movements, quickly moving away from the place, leaving the object immediately, etc.).

Cordon:

1. Do not allow bystanders to enter the area of the object left behind.
2. Try to identify the potential danger based on the external characteristics.
3. If, based on the analysis of the information received from the monitoring and the external characteristics of the object, it appears to be a dangerous object, follow the "call" procedure below.

Call:

1. Inform your superiors at each stage of the procedure.
2. Inform the necessary personnel of the HCC about the situation.
3. If a threat is identified, follow the crisis management chain of the security manual.

Control:

1. Control at every stage of all safety-related activities and the adequacy of the procedures carried out.

18.4. Parcels/letters

General description

All parcels delivered to the HCC should be hand-delivered or delivered via the parcel reception/distribution point at a designated point.

Deliveries should be avoided by being left unattended and should be advised and inspected when received. In the case of a heightened terrorist threat, any parcel left unattended should be treated as a suspicious item.

Response to the threat

The following procedures for handling correspondence and parcels are practical guidelines for all HCC staff.

- Incoming correspondence and packages: All correspondence and parcels (including personal), should be checked to verify the addressee and sender.
- Mail and parcels considered to be suspicious: Any consignment or package should be considered suspicious and requires special handling if:

1. A fictitious or unknown sender has been identified.
2. Indicates signs of leakage of a suspicious substance (liquid).
3. An unknown powder or granular substance is spilled.
4. Contains unusual wording (including threats).
5. Comes from an unusual and unexpected source or location of the sender.
6. Parcels with protruding wires, emitting an unusual smell.
7. Packages emitting a sound.
8. Packages containing unusual perceptible objects.
9. Packages of unusual weight.
10. Recipient's name is missing - only the position.
11. No return address.
12. Excessive number of stamps.
13. Linguistic errors.
14. Unusual inscriptions like: "To be sent by hand", “Personal!”

If one of the above points has occurred, put the consignment down (preferably outdoors or in a less sensitive location for the facilities) and notify the manager.

If you are suspicious about a package, it is advisable not to open it.

When you have not opened a package/parcel and it seems suspicious to you:

1. Handle it with care.
2. Do not shake or bump it.
3. Do not open, smell, touch or taste it.
4. Call to security.

This section applies if the parcel has been opened and the person opening it had or may have had direct contact with a potentially dangerous substance.

When you have opened a parcel containing an unknown substance (powder, granules, 'oily' substance, liquid):

1. Put the parcel down.
2. Inform the nearest personnel of the situation, at a safe distance (activating chain of alert).
3. Secure or cover it (e.g. with a plastic rubbish bag and adhesive tape or other

appropriate measures).

4. Turn off ventilation and air conditioning, close windows if they are open (to eliminate movement and air exchange).
5. Ensure that no one else approaches the location of the dangerous consignment.
6. Walk to the nearest room with running water.
7. Remove jewellery, and watch from your hands, put away your phone if you used it after opening the consignment.
8. Wash your hands very thoroughly using detergent or soap and rinse your hands with water for about 1.5 minutes.
9. Stay in the room until the appropriate emergency services arrive.

If you are sure or just suspect that a potentially hazardous substance may have been found on your clothing, then:

1. Put on disposable gloves.
2. Take out and unfold the plastic bag for rubbish.
3. Step onto the bag and remove any clothing contaminated with the hazardous substance.
4. Do this very carefully so that you do not touch your body with the contaminated clothing.
5. Put your previously removed watch and jewellery in it, your phone if you used it after opening the hazardous parcel.
6. Close the bag and put it in another bag and close it.
7. Remove gloves very carefully so that the outside of the gloves, do not touch your body.
8. Throw the gloves into a waste bin.
9. Wash hands very thoroughly with detergent or soap, and rinse hands for 1.5 minutes with water.
10. Move to another "clean" room and close the door behind you.
11. Do not eat, drink, or smoke.
12. Make a list of people who have had contact with the parcel.
13. Observe exposed parts of your body for redness, swelling, rashes, and itching, and observe for breathing problems, dizziness, and nausea.
14. Try to stay calm and rational.

18.5. UAV

General description

Technological developments have made flying drones (unmanned aerial vehicle – UAV) more common in everyday use. Until recently, they were used for entertainment, while over time they began to find application in various areas of life or industry, as well as for military or terrorist purposes, where they serve as platforms for reconnaissance, the carrying of warheads, or improvised explosive devices.

With the use of this device, it is possible to reach places that are difficult to access and are protected from unauthorized access, so it is necessary to anticipate the possibility of defending against such an attack in order to minimize its effects. Ease of operation, access, and low cost make them the perfect platform for dispersing CBRN agents in terrorist attacks. Specialized agricultural equipment seems ideal for this type of application.

They can disperse any type of aerosolised agent in a short period of time.

Transport by air bypasses any security of open spaces in an HCC and counter-measures are expensive, difficult to apply and relatively easy to avoid. Since air intakes are located on rooftops in most facilities and these are well protected from third-party access, the use of a drone may be the only way to deliver a CBRN agent to these facilities. The use of this dispersal mean is also additionally desired by terrorists due to the anonymity, safety of the perpetrator himself and the minimal number of people required to carry out the attack. The attacker is able to carry out an effective attack alone from a safe distance and his location is extremely difficult to detect and difficult to protect against.

Response to the threat

It is recommended that the HCC security should be provided with a procedure related to UAV incidents. That actions should be as simple as possible and can be requested only during the VIP's stay or for the duration of the event:

1. Creating a no-fly zone for UAV flights in HCC premises.
2. Securing sensitive installations (like air intakes) against the possibility of intentionally dispersion on dangerous agents (i.e. by installing protective nets).
3. If a UAV is observed outside the facilities but within its boundaries (e.g., above the roof, or inside the building), it is recommended to:
   - Observe the movements of the UAV.
   - Observe whether the UAV is carrying an attached payload.
   - Whether gas, powder or liquids is dispersed.

- Pay special attention whether UAV is approaching the air intake.

4. If the UAV is in the interior area of a building, warn its occupants about the danger (due to technical conditions, it may lose radio connection and crash in a random place.
5. Notify the police.
6. Try to find the UAV operator (physically and by CCTV).
7. If the person is found, and the area is no-fly zone, ask them to stay until the police arrival.
8. Implement the measures requested by VIP security

18.6. Vehicle

General description

Vehicle-related hazards range from accidents to use in terrorist attacks. The vehicle, due to its ability to transport significant quantities of dangerous agents, is considered to be one of the most likely sources of delivery large amounts of hazardous substances. Due to its mass and momentum, it can additionally serve as a tool to make a passageway at access points that are not protected against this type of attack and to ram people, thus increasing the number of victims of an attack.

Factors that increase the possibility and effectiveness of such an attack are:

- Freedom of movement near the HCC and the proximity of car parks to the facade of the facility.
- Location of assembly points after evacuation in the car parks.
- Underground car parks - a trap for vehicle evacuees.
- Weak anti-terrorist security at entry points before vehicles enter the area.
- Anonymity - theft or rental of a vehicle.
- Additional possibility of attacking people increasing the effectiveness of the attack.
- Possibility of destroying technical installations (e.g. gas pipes, electrical stations).

Response to the threat

Threats from vehicles can be mainly mitigated by installing technical/anti-terrorist security measures that can passively or actively protect key elements of the HCC against this type of

attack. These measures can be installed either permanently or temporarily in the case of an increased risk of a terrorist attack.

If a situation occurs where a door or other access point to the HCC is rammed and a vehicle enters the place, it should be considered that it could be a common accident, as well as a terrorist attack using CBRN means. This type of incident should always be approached with great caution.

In the first place, particular attention should be paid to:

1. Type and circumstances of the incident.
2. The symptoms of the injured person.
3. Your own state of mind (you feel dizzy, nauseous).
4. Gases coming from the vehicle, odours.
5. Other items that may indicate an attack with CBRN agents (canisters, containers, barrels).

If the incident has the appearance of a terrorist attack using CBRN agents then follow the general security procedures and initiate the notification and information process in accordance with the safety grid.

The facility security manager, once the above information is received, should immediately decide to evacuate the facility and inform the emergency services about the situation.

If possible:

1. Move to a safe location (downwind, out of the affected area).
2. Immediately notify the security officer and the police.
3. Protect the area from access by other people.

18.7. Ventilation system

General description

The mechanical ventilation system ensures that, regardless of weather conditions, fresh air is constantly supplied to the rooms, and used air is removed. Depending on the size of the building, it can function as a single system or a network of independent units.

The system is potentially exposed to hazards caused by the spraying of chemical or biological

substances or suspensions emitting ionizing radiation. Adequate protection of access to the technical space guarantees that equipment and the transmission network are always kept out of the immediate risk of contamination.

The most exposed components would include air intakes, air handling units and transfer ducts. In many existing buildings air intakes are located below or at ground level. It is beneficial to locate air intakes at the highest practical level of the building.

In order to protect against malicious activities, air intakes should be shielded by screens to prevent materials and other hazardous and dangerous substances from being placed, thrown or sprayed into them by a drone. Such screens should be sloped so that thrown objects can roll or slide off the screen, away from the intake. Some facilities have multiple ventilation zones, each operated by its own air handling unit and duct system. In practice, these zones are not completely separated if they are on the same floor. Air flows between the zones through corridors, vestibules, and doors, which are usually left open. Isolating separate ventilation zones minimize the potential spread of airborne hazards within the building and reduces the number of people potentially exposed in the event of a CBRN agent release.

Response to the threat

Considering the above, attention should be paid to:

1. Securing air intake locations to prevent unauthorized access:
   - Physical surveillance.
   - CCTV surveillance.
   - Motion detectors.
   - Access control system.
   - Unauthorized entry detectors.
2. Securing air intakes against the possibility of intentionally injecting toxic substances.
3. Installation of dangerous gas detectors.
4. Consider CCTV or physical monitoring of the critical ventilation system components during VIP visit

18.8. Technical installations

There are a number of technical installations such as gas, electricity, fuel, and other installations within the HCC. These installations can be used directly or indirectly to carry out

a terrorist attack using CBRN means. An important element is the need to locate the sensitive points of these installations vulnerable to terrorist attacks and to secure them accordingly.

The main efforts should focus on the technical security of the area against unauthorized access. This should be preceded by a security audit carried out by specialized companies, paying particular attention to gas and oil installations to identify unauthorized access and potential vulnerabilities. Appropriate measures should then be designed and implemented to protect these installations from damage or from being used in an attack.

GAS INSTALLATIONS

General description

The popularity of gas installations has a not-inconsiderable impact on the safety of buildings. Natural gas is a mixture of gases and various chemical compounds (e.g. odorous). However, regardless of its physical and chemical properties, when mixed with air the gas forms an explosive mixture. Just how dangerous this is, is confirmed by the many accidents and building disasters caused by gas leakage. The use of the existing gas installation in HCC has an impact on the operation of the building itself and many other business activities. Natural gas installations are vulnerable to intentional damage or terrorist attacks using explosives, or other factors that could create an explosion or fire.

An important consideration is the safe design of the installations within the facility itself, to avoid the placement of pipes in the immediate vicinity of hazardous material storage. Malicious actions can cause not only a space explosion of gas but also lead to the dispersion of hazardous chemicals such as: chlorine or ammonia. Another type of threat is cyber-attacks, which, as a result of receiving remote access to the control system, can take control of the proper operation of the installation and thus reduce the security of the facility. Cyber threats can arise both from the actions of terrorist hackers and as a result of sabotage carried out by employees with access to control systems. This threat requires particular attention to be paid to the verification of key personnel with access to the access protocols of ICT (information and communication technologies) systems for the management of sensitive technical installations.

Response to the threat

The minimum list of appropriate safety control measures for natural gas installations includes:

1. Documenting security procedures and maintenance activities.
2. Installing physical and logical access controls to cyber assets.
3. Authentication of authorized users.
4. Secure design of technical infrastructure networks.

5. Constant supervision of the maintenance of the installation by verified operators.
6. Use of pressure gauges and sensors to identify gas concentrations.
7. Make examination of gas lines a mandatory point of pre-VIP visit check

WATER INSTALLATIONS

General description

Water infrastructure, along with the technology required for its daily operation, is considered one of the critical elements of technical infrastructure. The target of attacks on water infrastructure can be direct damage to water purification or delivery systems. In this way, it can be contaminated by injecting poisons, pathogenic organisms, or chemicals into the distribution systems.

Water installations include:

- Distribution of drinking water.
- Purification.
- Storage.
- Sanitary systems.
- Heating systems.
- Fire-fighting systems.

Access to points in the system where chemical or biological agents can be introduced in HCC, in sufficient quantities to cause large-scale health risks, is usually limited. In addition, where water purification is employed, the range of chemical compounds is under strict control. Where biological agents that are resistant to treatment processes are used, there is the potential for poisoning the water.

Treated water is usually distributed to end users via distribution systems under high pressure and often inside technical zones. Although the main function of pipelines is to transport water, the pressurized nature of the network can prevent the possibility of injecting unwanted substances.

In buildings such as HCC, the supply is not directly from the distribution network but from local reservoirs and pressure towers above the level of the consumers. The final distribution to users via an independent pipeline network is often supplied by gravity at a lower and more stable pressure. The purified water in these reservoirs and towers is not under pressure and can therefore be more vulnerable. Tanks in HCC are also used as an integral part of sprinkler

and hydrant systems, which can be used to supply decontamination lines.

Response to the threat

1. Installations and their critical components should be installed in secure technical spaces, out of the access of unauthorized persons.
2. Critical points of the installation should be supervised by technical and physical surveillance systems.
3. Technical staff must be verified in terms of safety, qualification and experience.
4. Adequate procedural supervision should be in place for the maintenance and servicing of the installations (all maintenance work carried out by an external entity should be announced and supervised).
5. Staff of the HCC should be alert to unusual activities in the area of these installations and report them.
6. Separating different parts of the water distribution system improves control and allows the rapid isolation of suspicious or contaminated parts of the system.
7. Consider frequent water quality monitoring when VIP guests are present

18.9. External threats

Dangerous goods are substances and chemical compounds transported by public routes of communication. If HCC is located near a transport corridor whether road, rail or aquatic the accident in traffic or incident of malevolent origin may impact the facility. The fact of possible traffic accident should be reflected in the hotel emergency plan. That plan should be expanded by a component pertaining to the presence of VIP. The details of that component are placed in the order of matter in the text of this document.

Similarly, hazardous chemicals are used in many industries, in production and storage. . The HCC must be aware that many industries use chemicals, not only large chemical industries. An accident may occur as a result of a technical failure, but also intentionally through sabotage or a terrorist attack.

The zone of influence of some measures, depending on weather conditions and the type of incident, can reach up to several kilometres. Therefore, such risks must be taken into account in the security plans and instructions. The most important factors determining the radius of the impact of a hazardous cloud are quantity of hazardous material, wind strength and direction, temperature, and dispersion method.

Since any significant new processes involving hazards are subject to the authorization, HCC management should most likely know about aby existing or emerging hazards. Every such situation and its change should trigger an appropriate change in the emergency planning, in particular in its CBRN component.

A key element in improving safety is the development of an appropriate response plan. Those responsible for organizing safety should liaise with the institutions responsible for managing the transport of hazardous materials in the area and establish cooperation with industrial plants. Only close cooperation will allow the development of an appropriate and effective plan.

When analysing and responding to these risks, take into account the following:

1. Type of industry and possible risks associated with it.
2. Type of transport mode in the vicinity of the site (road, rail, inland waterway, air).
3. Distance and direction from these points.
4. Include exposure mitigation in emergency planning
5. Establish a point of contact for exchanging information on the risk with nearby facilities and relevant services.
6. Carry out systematic training related to the implemented procedures to counter the risks.

18.10. Negotiating protocol in case of CBRNe VIP event

Developing a negotiating protocol for CBRNe VIP events in HCC involves establishing clear procedures and guidelines for communication, coordination, and decision-making in the event of a CBRNe threat or incident involving VIP´s.

Knowing the difficulty in completely avoid the occurrence of an attack with CBRN agents, the focus on minimizing these risks must be on prevention. In the case of HCC, prevention is associated with the prior detection of these possible attacks, failing to prevent or detect them, measures must be implemented to mitigate their effects, also creating specific protocols that allow an adequate response so that the normality is restored as quickly as possible.

To develop the measures listed below, local LEA´s must be consulted, mainly the services with capabilities and experience in the security of large events and the protection of VIP’s as personal or close protection police services. The HCC must take into consideration the following action listed protocols to protect VIPs at CBRNe events. For outdoor or open-door

events, all measures mentioned must be implemented, with the necessary adaptations.

19. Pre-Event planning

Prior to the VIP visit a person nominated by the HCC manager should arrange an advanced security meeting. This is very important to define the hotel location assigned to the VIP and allocate staff resources to support them, knowing the pre-established plan for the specific visit. In case of the lack of time such meeting may happen during pre-visit briefing. One of the two events is mandatory in VIP visit preparation.

19.1. Content of the VIP visit advanced security meeting

In a pre-security meeting for a VIP visit to a HCC, particularly when considering CBRN threats, several critical areas should be covered to ensure a comprehensive security strategy.

- VIP Profile & Threat Assessment:
  - ✓ VIP Background. Discuss the identity, status, and any specific requirements of the VIP.
  - ✓ Threat Assessment. Review intelligence on potential threats (CBRN threats, previous security incidents involving the VIP and known adversaries or high-risk groups).
  - ✓ Risk Level. Classify the event or visit's risk level (low, medium, high) based on this assessment.
- Security Plan Overview
  - ✓ Security Zones. Identify high-risk, medium-risk, and low-risk zones within the HCC.
  - ✓ Layered Security. Discuss the outer, middle, and inner perimeters of security, including checkpoints, surveillance and access control measures (badges, escorts, etc.).
- CBRN Preparedness
  - ✓ Detection Systems. Review systems in place for detecting chemical, biological, radiological, or nuclear agents, including air and water filtration.
  - ✓ Response Protocols. Discuss protocols if a CBRN threat is detected: Immediate lockdown measures, evacuation routes and safe zones (if contamination is suspected), decontamination procedures.
  - ✓ Medical Resources. Identify available medical support, CBRN-specific treatments, and nearby facilities capable of handling such emergencies.

- HCC Security Infrastructure
  - ✓ Surveillance. Confirm the functionality of CCTV, monitoring systems, and integration with LEA.
  - ✓ Security Staff. Review roles and responsibilities of the security personnel on-site: CBRN awareness and response training and assignment of key personnel to critical areas.
  - ✓ Access Control. Ensure restricted access to VIP areas, the use of metal detectors, baggage screening, and potential CBRN detection equipment.
  - ✓ Visitor Screening. Discuss methods for screening guests, vendors, and staff for potential threats, including the use of detection equipment and protocols.
- Contingency & Emergency Plans
  - ✓ Evacuation Protocols. Ensure clear plans for a swift evacuation in case of an incident, including both general security and CBRN-specific routes.
  - ✓ Alternative Routes/Exits. Map out alternative routes and exits in case primary ones are compromised.
  - ✓ Communication Systems. Ensure reliable communication systems (e.g., radios, encrypted phones) are in place for use during an emergency.
  - ✓ Coordination with First Responders. Confirm pre-arranged coordination with local law enforcement, emergency services, and CBRN response units.
- Cybersecurity
  - ✓ HCC Infrastructure Protection. Ensure the protection of the HCC's IT systems from potential cyber-attacks, which could disrupt communications or manipulate security systems.
  - ✓ VIP Information Security. Safeguard any personal or itinerary information about the VIP to prevent it from being leaked or exploited.
- Coordination with HCC Staff
  - ✓ Briefing HCC Staff. Review the level of involvement of staff, ensuring they are briefed on security protocols and aware of how to handle suspicious situations.
  - ✓ Discreet Operations. Emphasize the importance of discretion among HCC staff to avoid unnecessary attention or leaks of sensitive information.
- Media and Public Relations
  - ✓ Media Management. Plan for managing the media presence if relevant, and ensure that no security vulnerabilities are created through media exposure.
  - ✓ Public Interactions. Discuss the strategy for managing any scheduled public

appearances or interactions to avoid security breaches.

- Final Walkthrough
  - ✓ Venue Walkthrough. Conduct a final walkthrough of the venue to ensure that all planned security measures are in place and working as expected.
  - ✓ Drills/Exercises. If time permits, conduct security drills to ensure everyone knows their role in case of an emergency.

By covering these areas, the pre-security meeting ensures a coordinated and proactive approach to safeguarding the VIP, HCC staff, and guests from both general security threats and CBRN-specific threats.

19.2. VIP visit

As soon as the reception of a VIP at a hotel or the organization of an event with VIPs is confirmed, the person responsible for security should work on the following ideas to increase security levels and avoid the possibility of a CBRNe incident:

- Designate a dedicated security liaison or team responsible for coordinating security arrangements for CBRNe VIP events.
- Designate dedicated staff to be responsible for the VIP security area.
- In hotels, take into account the location of the room assigned to the VIP, giving preference to a room:
  - On an isolated floor (or without occupants in neighbouring rooms, leaving the possibility that these adjoining rooms could be used by the security team, who must have an alternative and direct passage to the VIP's room);
  - ✓ Easily reachable by emergency services;
  - ✓ Located in a reserved or isolated area of the hotel (far from the hotel's common areas: bars, restaurants, etc.) and with a minimum of two escapes routes;
  - ✓ With independent ventilation;
  - ✓ Preferably with at least two access possibilities (separate entry/exit point);
  - ✓ With a wide view and without nearby buildings (avoid access through balconies or windows).
- If the room does not meet the conditions mentioned before, the room should be located in the "safe house" area.
- The security team must ask to have in their possession alternative keys for all the

facilities that the VIP could be access;

- In places that will be used by VIPs, ensure that the space is thoroughly cleaned before the VIPs arrive, in which all surfaces must be cleaned with disinfectant products, paying special attention to surfaces that come into most contact with hands (door handles, doors, television controls, light switches, etc.).
- In common areas, if possible, keep a dedicated toilet exclusively for VIPs;
- Keep a dedicated elevator for VIP, if possible (more than one);
- Request LEA to carry out CBRNe security searches.
- During these security searches, pay special attention to the items in the spaces that will be used by VIPs:
  - ✓ All fabric items, such as towels, sheets, cushions, and napkins, must be guaranteed intact from hot washing and ironing to the final destination.
  - ✓ All packaging such as shampoos, shower gels, water bottles, or other containers with liquids must be properly sealed and an inspection must be carried out (for example, squeezing the packaging) to confirm that there is no leak in the packaging (an indication that it may have been injected something inside).
  - ✓ In toilets, (if possible, have a dedicated one exclusively for VIP) pay particular attention to pedal waste bins, flush toilets, and taps, confirming and testing their correct functioning. Toilet paper, as it is an item that comes directly into contact with the mucous membranes of the human body, must be discarded at least the first third of it.
- When carrying out these searches, all available equipment must be used to detect CBRNe threats, if possible, using more than one piece of equipment for each of the threats (chemical, biological, radiological) and preferably using different detection technologies.
- After carrying out the security search, implement a security perimeter that guarantees that nothing enters it without being previously inspected.
- If allowed for local legislation, install surveillance cameras for control access to the place where the VIP is installed (through dedicated security teams);
- Control the loading and unloading HCC area, checking everything that enters the facilities in the days before the event or the VIP arrival.
- Check the emergency exits and, if possible, install the VIPs in a location that may have one of these emergencies exits reserved for the exclusive use of the VIP entity.
- Inform police intelligence services for assigning degrees of threat to the event and the level of risk associated with the VIPs involved.

- Vetting all employees and staff involved, with a special focus on recently hired ones.
- Conduct thorough risk assessments and develop contingency plans for CBRNe threats, considering potential scenarios and response measures.
- Checking and guarantee the correct functioning of critical infrastructures, namely electricity panels and elevator systems, requesting a 24-hour technician support and ensure the possession of master keys that allow access to all parts of the HCC facilities.
- Establish communication channels and protocols for rapid dissemination of information to relevant stakeholders, including event organizers, VIP security, hotel management, hotel security personnel, and emergency responders.

20. During the event

During the event, the security manager should implement, if needed with the cooperation of VIP Security, measures to reduce the possibility of a CBRNe incident:

- Ensure the controlled entry of all employees, identification and objects (using gantry and X-ray).
- Implement a 24-hour facility security perimeter around the HCC.
- Control the place's video surveillance cameras.
- Non-essential parallel businesses should be closed (bars open to external customers, hairdressers, SPA, etc.).

But it is important not forget that the main measures to be implemented so that the VIP's stay and the event run smoothly do not just start on the day of the event, but rather through the creation of daily and permanent routines that ensure that all venue staff are constantly alert through the application of the previously mentioned prevention procedures.

The HCC security manager must ensure this permanent alert by communicating to the VIP security teams any abnormalities that have recently been detected.

21. Reaction in case of CBRNe event

The following procedures are some of the measures that can be implemented if we suspect or are faced with a confirmation of a CBRNe attack. The steps listed do not have a specific order and can be carried out simultaneously.

- Follow the 1-2-3+ process to judge what actions the situation requires.
- Evacuate the VIP (or shelter in place). The decision will always be made in partnership between the HCC security manager and the VIP security officer, one decision can never contradict the other. Select the type of evacuation (or shelter in place).
- Recognition of evacuation routes (pre-established and prior knowledge of security teams).
- Selection of the safest evacuation route (main or backup).
- Use the PPE available (if possible). In this case, the most recommended PPE is the escape masks for VIPs and the gas masks for those responsible for security or evacuation. Even if there is more PPE available, the risk of wasting time to equip it, plus the possibility of it not being well sealed, increases the risk of contamination for the user, making it easier and safer to leave the location with an escape mask or mask, and implement de REMOVE procedures when in a safe place.
- After arriving at the evacuation point previously established in the security plan, remove the VIP to a safe location (normally using a vehicle dedicated to the VIP).
- Give the alert.
- Communicate with LEA (METHANE).
- Implement procedures (REMOVE).
- Conduct a search operation (with guidance from LEAs).
- Initial decontamination procedures. Decon kit for VIP and close protection team, mainly against chemical threat (products very easy to use).
- Cleaning surfaces procedures (supported by LEA’s specialized teams).

22. Conclusions and recommendations

Creating a dedicated CBRNe protection program in HCC is extremely important to increase the security of all people who use these places, soft targets often frequented by high-level personalities or VIPs during their stays in hotels and participation at conferences and events.

As presented in this report, the best way to mitigate the possible effects of a CBRNe event is to invest in prevention, in order to have the necessary tools to detect and react to the possibility of a CBRNe incident, namely, having all staff alert and prepared for these threats, implementing internal control measures for people, objects and infrastructures, establishing communication and response protocols with local LEAs, and implementing all necessary security measures that can help in detecting these threats. If, even with these procedures, the HCC are faced with a CBRNe event, they must be prepared to evacuate everyone and inform them about the expeditious decontamination actions to be carried out until the arrival of specialized security teams.

An easy way for end users of this project to remember these measurements is through the following mnemonic "Staff Carefully Plans Security Every Day ", where each initial sentence letter corresponds to the following procedures:

- S - Staff Training.
- C - Control (people, objects and infrastructure).
- P - Protocols with LEA.
- S - Safety and security measures.
- E – Escape.
- D – Decontamination.

This phrase captures the essence of daily vigilance and planning required to ensure safety and security in HCC.