



Safe Cities

Deliverable D2.4

SAFE-CITIES SVA framework



Due date of deliverable: 31/10/2023

Submission date: 03/12/2023

Dissemination level		
PU	Public	X
SEN	Sensitive	

Start date of project: November 1, 2022

Duration in months: 26

Consortium partners

STAM SRL	Italy
IANUS CONSULTING LTD	Cyprus
ALMA MATER STUDIORUM - UNIVERSITA DI BOLOGNA	Italy
D-VISOR BV	The Netherlands
NATIONAL CENTER FOR SCIENTIFIC RESEARCH "DEMOKRITOS"	Greece
STOWARZYSZENIE POLSKA PLATFORMA BEZPIECZENSTWA WEWNETRZNEGO	Poland
ISTITUTO DI SOCIOLOGIA INTERNAZIONALE DI GORIZIA ISIG	Italy
CONFEDERATION OF EUROPEAN SECURITY SERVICES	Belgium
COMUNE DI GORIZIA	Italy
POLIISIHALITUS	Finland
STADSREGIO PARKSTAD LIMBURG	The Netherlands
MESTNA OBCINA NOVA GORICA	Slovenia
<i>Fondazione per l'Innovazione Urbana*</i>	<i>Italy</i>
ASSOCIAZIONE CROCE ROSSA ITALIANA COMITATO DI GORIZIA	Italy
MINISTRY OF INTERIOR	Cyprus
PROVINCIAL POLICE HEADQUARTERS IN GDANSK	Poland
MINISTRSTVO ZA NOTRANJE ZADEVE	Slovenia
THRIDIUM LIMITED	United Kingdom
UNIVERSITA VERDE DI BOLOGNA APS	Italy

**Terminated*

Document control sheet

Deliverable number	D2.4
Deliverable responsible	NCSR
Work package	WP2
Main editor	Athanasios Sfetsos (NCSR)

Editor name	Organisation
A. Sfetsos, Y. Tsourounakis	NCSR
D. Longo, F. Sabatini, S. Orlandi, M. Massari, B. Turillazzi	UNIBO
S. Mieszczak	KWPG
M. Wolbach	PPHS
J. Puustinen, D. Breucha	NPB
A. Frank	COESS
R Coceancig	CRI-GO
U. Battista	STAM
E. Barri, G. Kioumourtzis	IANUS
P. Veltsistas	TEL
M. Muzzatti, L. Sacellini	CGO
R. Velea	ISIG

Document revision history			
Modifications introduced			
Version	Date	Reason	Editor
D1	23/08/2023	TOC	A. Sfetsos (NCSR)
D2	3/10/2023	Public Private Partnerships	COESS
D3	26/10/2023	Security by Design	UNIBO
D4	30/10/2023	Citizen Engagement	ISIG

D5	29/11/2023	SVA update	All partners
D6	30/11/2023	Review	IANUS / STAM
D7	03/12/2023	Final version	NCSRD

Disclaimer

This report was prepared as an account of work funded by the European Commission. The contents of this document are provided “AS IS”, and no guarantee or warranty is provided that the information is fit for particular purposes.

The information, analyses and views set out in this report are those of the author(s) and do not necessarily reflect the official opinion of the European Union. Neither the Community institutions and bodies, nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein. The user, thereof, uses the information at its sole risk and liability.

Copyright notice

© 2022 – 2024 SAFE-CITIES Consortium

Abbreviations and acronyms

CAD	Computer Aided Design
CAPEX	Capital expenditures
CBRN	Chemical Biological Radiological Nuclear
CCTV	Closed Circuit TV
CoESS	Confederation of European Security Services
CPTED	Crime Prevention Through Environmental Design
D	Deliverable
DBT	Design Basis Threat
ENLETS	European Network of Law Enforcement Technology
ER	Emergency Response
EU	European Union
EU-VAT	EU - Vulnerability Assessment Tool
FR	First Responders
GDPR	General Data Protection Regulation
GIS	Geographical Information Systems
IED	Improvised Explosive Device
LEA	Law Enforcement Agency
NEB	New European Bauhaus
NGO	Non Governmental Organization
OPEX	Operational Expenditures
OPSEC	Operations Security
PBIED	Person Borne IED
PDA	Personal Digital Assistants
PPS	Physical Protection System
SSH	Social Sciences and Humanities
SVA	Security and Vulnerability Assessment
TTX	Table Top Exercise
UAS	Unmanned Aircraft Systems
UAVIED	Unmanned Aerial Vehicle IED
VA	Vulnerability Assessment
VBIED	Vehicle Borne IED

Contents

Abbreviations and acronyms.....	6
Contents	7
Executive summary	10
1. Introduction	11
2. SAFE-CITIES SVA : Scope and Methodology for establishing.....	13
2.1. SVA framework within SAFE-CITIES	13
2.1.1. EU public space protection policies	13
2.1.2. Scope of the SAFE-CITIES SVA	14
2.2. SVA development and validation process.....	16
2.2.1. Gdansk Workshop.....	16
2.2.2. Larnaca Workshop.....	17
3. SAFE-CITIES SVA – Key updates from D2.1	19
3.1. Incorporation of the public – private partnerships.....	19
3.2. Incorporation of LCN	19
3.3. The ATLAS framework for introducing security by design solutions.....	19
3.4. Update of the SVA	19
4. The Security by design concept in the SAFE-CITIES SVA	21
4.1. The concept of public space in the SAFE-CITIES project.....	22
4.2. Urban design principles for Safe Public Spaces: theoretical framework.....	24
4.3. 'Atlas – 4 safe public spaces design guiding framework'	28
5. The role of public – private partnerships the public space protection	34
5.1. The European Commission's Good Practices to support the Protection of Public Spaces" and Recommendations for public-private collaboration.....	35
5.2. Views of the European private security services industry: state of play of public-private collaboration for the protection of public spaces	36
5.2.1. The precondition: national regulation on private security tasks and competencies in public spaces	37
5.2.2. Added value of private security in the protection of public spaces	38
5.3. Framework for public-private collaboration and Joint SVAs.....	39
5.4. Recommendations and guidelines of the private security industry for enhanced public-private collaboration	41
6. The SAFE-CITIES SCPM within SVA.....	44

6.1.	Introduction	44
6.2.	Local Citizens Networks (LCNs)	44
6.2.1.	LCN Structure	45
6.2.2.	Engagement Strategies.....	45
7.	The SAFE-CITIES SVA	46
7.1.	Step 1. Identify the SVA Team.....	46
7.2.	Step 2. Plan the SVA.	48
7.3.	Step 3. Define the Threat vector.....	49
7.3.1.	Identification of adversary registry	49
7.3.2.	Characterization and ranking of adversaries.....	50
7.3.3.	Implementation of the design basis threat (DBT)	51
7.3.4.	Emerging Threat landscape – Unmanned Systems	52
7.4.	Step 4. Characterization of the public space	54
7.4.1.	Categories of Public Spaces of relevance to SAFE-CITIES.....	55
7.4.2.	“Open”, “semi-open” or “closed” spaces.....	56
7.5.	Step 5. Identify the Targets and quantify their attractiveness.....	56
7.6.	Step 6. Describe the public space security system	57
7.6.1.	SAFE-CITIES public space security integrated policies functions	59
7.6.2.	PPS design considerations.....	61
7.6.3.	Counter UAS	62
7.6.4.	Community Policing.....	62
7.7.	Step 7. Conduct risk assessment.....	63
7.8.	Step 8. Scenario Building: Determine the most vulnerable path and develop worse-case scenarios	65
7.8.1.	Path analysis.....	66
7.9.	Step 9. Responding to the threat	67
7.9.1.	Attack Interruption and Neutralization	67
7.9.2.	Emergency Response Actions	68
7.9.3.	Radiological Event Response	72
7.10.	Step 10. Identify and Quantify vulnerabilities, determine areas for improvement, and propose upgrades.....	73
7.11.	Step 11. Re-evaluate public space with Proposed Improvements.....	76
7.12.	Step 12. Reporting, Training and Risk Communication actions	77
8.	SAFE-CITIES SVA Quantification.....	78

9.	SVA testing and evaluation protocol	79
10.	SVA integration within SAFE-CITIES software	80
11.	Conclusions	81
12.	References	82
13.	Appendix 1 – Existing good practices on public private partnerships in the field of public space protection	83
14.	Appendix 2 – Atlas 4 safe public spaces design guiding framework	92
15.	Appendix 3 – Design examples portfolio	93
16.	Appendix 4 – Testing the SCPM in pilot cities	105
16.1.	Case Study 1: Gorizia (IT) – Nova Gorica (SLO)	105
16.1.1.	Activities Performed	105
16.1.2.	Next Steps	105
16.2.	Case Study 2: Larnaca (CY)	105
16.2.1.	Activities Performed	105
16.2.2.	Next Steps	106
17.	Appendix 5 – Compliance-Based Vulnerability Assessment	107

Executive summary

D2.4 introduces the revised version SAFE-CITIES security and vulnerability assessment baseline framework (SVA). It has been the outcome of a meticulous process involving almost the majority of the consortium and external partners in six workshops and hackathons. The revised

The revised SAFE-CITIES SVA Framework introduces elements of “secure city by design” in the characterization of the public space using the ATLAS tools (Task 2.3), a parsimonious “citizen engagement” strategy supported by engagement tools (presented in D2.3) and a consolidated framework and recommendations for enhancing public-private cooperation. It reports the outputs from T2.3, T2.4 and T2.5.

The revisions made within this Deliverable, are based on the recommendations by external experts and consortium members in the workshops and hackathons were concentrated in three main steps of the initial SVA framework (D2.1). The final list of steps is introduced in the following lines, with bold letters indicating the revised ones.

1. Identify the VA team
2. Plan the VA **and define risk tolerance**
3. Define the threat vector
4. Characterize the public space
5. Identify the targets and quantify their attractiveness
6. Describe the public space security regime
7. Conduct risk assessment
8. Scenario Building: Determine the most vulnerable path and develop worse-case scenarios
- 9. Responding to the threat**
10. Identify and Quantify security vulnerabilities in public spaces
11. Re-evaluate the public space with proposed improvements
12. Reporting, **Training and Risk Communication** actions

The revised SVA has been fully aligned with the software tools and solutions that have been proposed in SAFE-CITIES and developed in WP3 and WP4.

1. Introduction

The European Union has engaged in a vast set of actions aiming to provide support to European urban environment and communities in order to maintain the highest possible standard of living and well-being. The European Council has already identified (EU Council 2021) the need to strengthen efforts for upgrading the protection of public spaces and open areas against terrorism attacks.

The rapidly changing security environment in the EU and beyond calls for the continuous enhancement of the capacities of European LEAs and local / national authorities. This includes expanding partnerships with the private sector and also the introduction of citizens, the development of a consolidated framework (SVA) covering all crisis phases – from planning to response –, innovative digital tools for processing vast amount of data, highly informative visualization tools.

These tools and concepts do not put security provisions as a stand – alone merit but integrate them with evidence-based urban design, planning and management measures, emphasizing measures to embed protective physical features and encourage prosocial behaviour through the design and management of a location of interest. Within SAFE-CITIES SVA the “security by design” approach (COM2017), is being used as a measure to increase security through the human centred design of public spaces, and public awareness campaigns as part of urban regeneration measures.

The majority of European public spaces and major events, such as religious / worship places, transportation hubs and stations, public and recreation parks / tourism sites, business areas, educational establishments, major sports and cultural events, mass gatherings etc, are potentially «high value» targets, exposed to different and diverge threats and each with unique vulnerabilities. Within SAFE-CITIES, an effort has been made to harmonise approaches and concepts for providing a harmonised and comprehensive approach to different public spaces and major events, that is presented in this Deliverable.

Following the recommendations of (COM2017), SAFE-CITIES SVA framework addresses in a holistic and integrated manner relevant strategies across institutional boundaries, public-private partnerships and citizen engagement process, urban design with advanced digital tools to support the SVA process. The main aim of the SVA is to provide a uniform security and vulnerability assessment methodology that can be followed by all actors involved in the security of public spaces. The proposed concepts solidify existing experience and knowledge in this challenging area and lays the groundwork for establishing a concrete methodology with the support of modern digital and AI/ML tools (WP 3, WP 4)

The final version of the SVA methodology provides a generalised set of implementation guidelines and recommendations for facilitating all responsible entities in following a structured step-by-step approach towards securing public spaces, starting with a

comprehensive assessment of the public spaces and the corresponding Vulnerability Assessment (VA), and leads to the selection and analysis of appropriate security solutions (including the by-design) and upgrades.

2. SAFE-CITIES SVA : Scope and Methodology for establishing

Chapter 2 introduces the basic principles of the SAFE-CITIES framework starting from an overview of the EU public protection policies and proceeds with a description of the scope of the SVA. The readers are directed to D2.1 for a comprehensive assessment of literature review and appraisal of past research projects and operational examples from the project partners from the respective case studies.

2.1. SVA framework within SAFE-CITIES

2.1.1. EU public space protection policies

The EU and its Institutions have engaged in multiple activities related to the Protection of the European citizens Table 1 presents related EU sources of information:

Table 1: Reference EU work for public space protection.

Title	Link
Council Conclusions on the Protection of Public Spaces (2021)	https://futurium.ec.europa.eu/en/urban-agenda/security-public-spaces/library/council-conclusions-protection-public-spaces
Action Plan to support the protection of public spaces COM/2017/0612 final	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017DC0612
A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond COM/2020/795 final	https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0795&from=EN
Good practices to support the protection of public spaces SWD(2019) 140 final	https://op.europa.eu/en/publication-detail/-/publication/998aeb09-4be6-11e9-a8ed-01aa75ed71a1/language-en
Security by Design: Protection of public spaces from terrorist attacks SWD(2022) 398 final	https://home-affairs.ec.europa.eu/system/files/2022-12/Staff%20working%20document%20-%20Security%20by%20Design%20-

	%20Protection%20of%20public%20spaces%20from%20terrorist%20attacks_en.PDF
JRC Science Hub	https://joint-research-centre.ec.europa.eu/scientific-activities-z/protection-public-spaces-terrorist-attacks_en
Handbook on UAS protection of critical infrastructure and public space	European Commission, Joint Research Centre, Hansen, P., Pinto Faria, R., Protection against Unmanned Aircraft Systems – Handbook on UAS protection of critical infrastructure and public space – A five phase approach for C-UAS stakeholders, Publications Office of the European Union, 2023 ¹

We close this section with copying the **definition of the VA** according to the EC SWD “Security by Design: Protection of public spaces from terrorist attacks” ... Vulnerabilities are the inherent weaknesses of a potential target that may render it susceptible to the destructive consequences of a terrorist attack. *Critically assessing vulnerabilities in the context of attack scenarios* will assist decision-makers in taking informed decisions on deterrence and mitigation measures, designing strategies to minimise exposure and developing an effective emergency management plan. A detailed examination of the asset under consideration *can identify deficiencies and flaws* that may encourage the formulation of an attack plan.

Clearly, vulnerabilities are closely related to the main function of each public space. ... Thoroughly identifying the vulnerabilities of a public space requires the examination of factors such as its accessibility, cultural/religious/symbolic significance, location, shape and existing protective measures (entry checks, video surveillance, security guards, perimeter protection, etc.).

2.1.2. Scope of the SAFE-CITIES SVA

The security of public spaces is based on the cooperation between LEAs, local authorities and the private sector, based on ad-hoc or locally established procedures. The SVA framework (Figure 1) was developed within the SAFE-CITIES project following an iterative process where project partners interacted between them in order to:

¹ <https://data.europa.eu/doi/10.2760/18569>

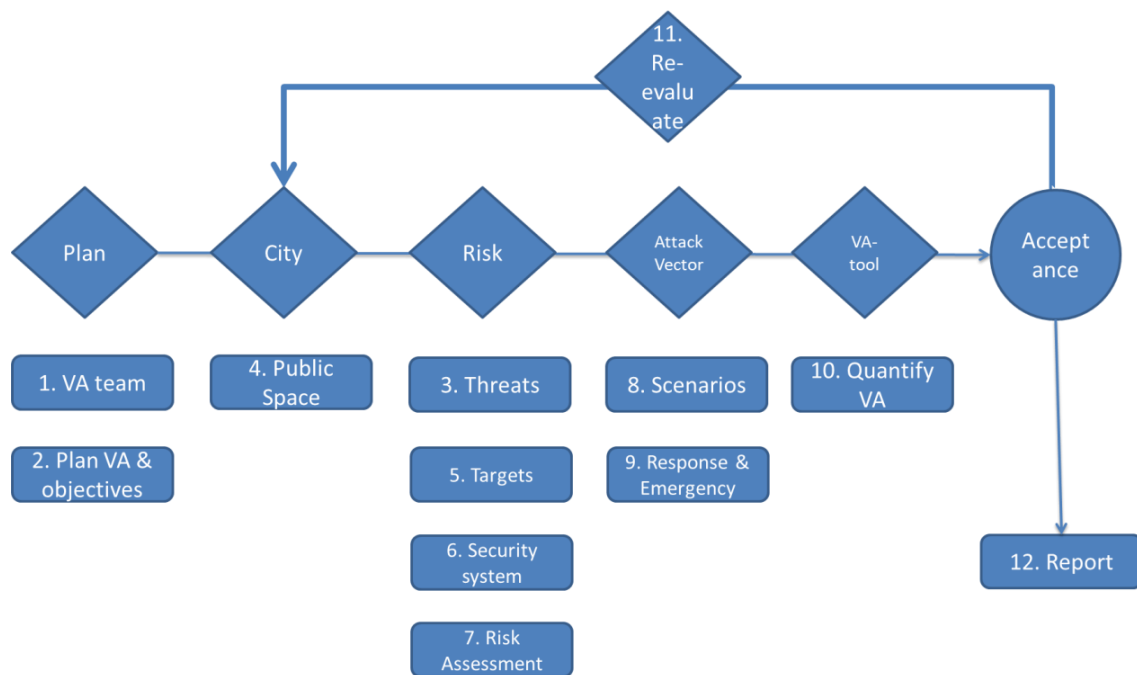


Figure 1: SVA Process diagram.

- understand the needs and requirements of public space protection frameworks,
- capture the operational experiences of the LEAs, emergency responders, municipalities and other authorities through targeted interactions,
- synthesize existing frameworks from the literature and operational experiences.

The SVA framework was assembled into a 12-step process (Chapter 7) build upon specific requirements as identified within the SAFE-CITIES workshops. They address key challenges in the security domain shown in Table 2.

Table 2: SVA key principles.

SAFE-CITIES philosophy in a nutshell
Single solution to account for all phases of security and emergency response actions
Consistency across normal conditions within urban environments and also mass gatherings / events
Multi-stakeholder partnerships, across the public and private sector
Citizen Engagement through local community networks
Support the “Security-by-design”, through the Crime Prevention Through Environmental Design (CPTED) concept
Seamlessly introduce conventional and also emerging threats such as UAS
SVA has a static and dynamic component

Vulnerability considers operational, technological and human aspects
VA is comprised of two elements: the static and the dynamic, considering the space breath and time of the scenarios.

2.2. SVA development and validation process

The SAFE-CITIES SVA process was developed with the project partners in a joint effort that started from M1 of the project. Initially **two internal workshops** were conducted with all partners to a) set up the guiding principles of the framework and b) discuss the SVA process.

Then the consortium presented the methodology in the Gdansk Workshop (M6) – section 2.2.1 - where external experts had the opportunity to interact and give feedback on the SVA.

This process was followed by two more internal, online, workshops where a) feedback from the Gdansk workshop was incorporated in the SVA, b) alignment of the SVA with the project's planned and new tools was made.

Finally the consortium presented the SVA methodology in the Larnaca workshop and hackathon – section 2.2.2 – introducing also the SVA tool in support of phases 1-7 of the methodology. Collected feedback and some fine-tuning was performed until the final version of the SVA has been incorporated in D2.4

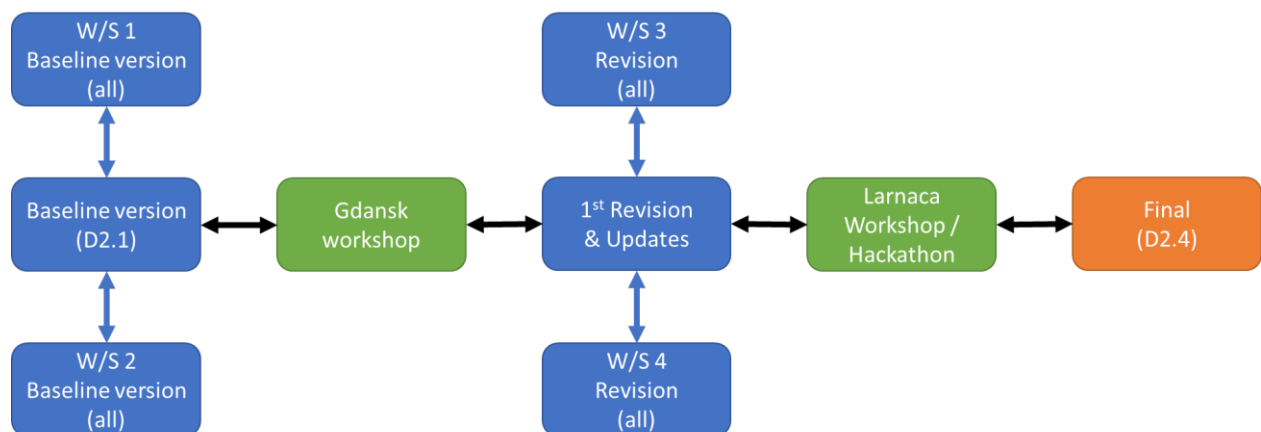


Figure 2: SVA Development process.

2.2.1. Gdansk Workshop

Security practitioners, responsible for the protection of public spaces, have been gathered in face-to-face workshop, organised by Polish Platform for Homeland Security, in Gdansk (May 2023) in order to use and test proposed SVA methodology

on pre-defined security scenarios: 1) Clashes/fights between fans several hours before the game at the Railway Station; 2) Clashes/fights between fans immediately after the football game started at the stadium in Gdansk; 3) Mass shooting terrorist attack during the Christ-mas shopping period; 4) CBRN attack during a high-intensity shopping day; 5) Suicide terrorist attack after the headliner concert; 6) Bombing attack using drones; 7) False bomb alert in a crowded square, and 8) Car driving into the crowd. The main objectives of the proposed tabletop exercises are:

- To apply the methodology to selected security scenarios;
- To define if the proposed methodology would have allowed security practitioners to prevent/anticipate the security incident defined? And how the risk would have been mitigated;
- To evaluate is the methodology: Comprehensive? Simple or Complex? Applicable to real-life situations;
- To identify the strengths and weakness of the proposed methodology;
- To propose practical improvements and/or define the areas for improvements.

Several groups have been formed, composed of different expertise and background in order to stimulate knowledge exchange and constructive discussions, and invited to apply the SVA methodology on two security scenarios. Several iterations took place, and group leaders shared and argued findings and recommendations with other groups. Finally, all feedback and recommendations have been collected for further processing and implementation; thus, contributing to the fine-tuning and enhancement of the SVA methodology.



Figure 3: Gdansk workshop.

2.2.2. Larnaca Workshop

A three-day meeting was held in Larnaca, Cyprus, in CYCLOPS Training Centre where the workshop and the hackathon for the evaluation of SVA platform took place where a total of 54 people attended the event. During the second day of the meeting, the platform was presented to both the consortium and external partners, the functionality and a brief demo provided the audience an initial idea of what to expect during the

hackathon.

On the third day of the meeting, attendees were divided into six groups of six members each. Each group consisted of both partners and experts (such as civil defence personnel, security officers, firefighters, policemen, representatives from the Metropolis Mall etc). In the first part of the hackathon, with guidance from NCSRD and IANUS, each group ran a test case using the platform to familiarize themselves with the tool. In the second part of the hackathon, the groups executed the scenario that had been pre-defined and distributed by PPHS. There were three scenarios in total, so two groups worked on the same scenario that helped to compare the results at the end of the hackathon.

- Scenario #1: Due to the main door renovation the entrance no. 1 (on the Car Park & Koritsas Street side) is closed
- Scenario #2 : Planned mass gathering (how many people?) advertising event inviting a very known influencer
- Scenario #3: National Terrorist Threat Level is raised to HIGH due to possible terroristic attacks using car-on-crowd

Each group, having received its respective scenario, was requested to respond to the SVA questions, corresponding to the information of their assigned scenario but with also the need of making some assumptions. In the end, each group presented its results, allowing for a comparison of each group's perspectives and how the results were influenced by the assumptions they made.

In addition to the outcomes, the attendees completed a platform evaluation questionnaire and pointed out areas that could be changed or modified in the platform. Users also mentioned what additional features could be included in a future version of the SVA tool.



Figure 4: Larnaca Workshop and hackathon.

3. SAFE-CITIES SVA – Key updates from D2.1

This chapter introduces the main updates of the SVA framework as it evolved from its initial version – introduced in D2.1 – to the present one. Briefly these are introduced in the following lines.

3.1. Incorporation of the public – private partnerships

Following the coordination of CoESS in Task 2.4, a set of recommendations was established how to improve public-private collaboration in Europe, which includes a multitude of trust and collaborative building culture, soft actions and technological solutions (Chapter 5)

Success criteria and respective recommendations from the private sector have been devised for the establishment of public-private collaboration, which can include joint SVAs and trainings.

3.2. Incorporation of LCN

D2.4 proposes the Incorporation of LCNs into each of the 12 SVA steps for enhancing community participation and achieving a holistic approach to public space security. By providing LCNs with specific communication and engagement tools and materials, SAFE-CITIES project empowers them to contribute effectively to SVA exercises.

3.3. The ATLAS framework for introducing security by design solutions

The 'Atlas 4 safe public spaces design-guiding framework' is an operational tool supporting the evaluation of some socio-technical aspects and features of the urban space which might not be considered in traditional security assessment tools.

3.4. Update of the SVA

Individual updates to the SVA included a) work on the understanding and assessing emerging threats with a focus on UAS and CBRN, b) adding the response dimension to the SVA process, where the radiological incidents had a separate chapter, c) adding the training and risk communication in step 12 and d) updating and reviewing

categories in the likelihood, impact, attractiveness and risk assessment process.

4. The Security by design concept in the SAFE-CITIES SVA

SAFE-CITIES project represents a necessary answer to the challenge of balancing both the protection and the accessibility/usability/openness of public spaces. It acknowledges the fact that urban and architectural design of these spaces should be pivotal in determining whether they enhance social safety or they create a vulnerable environment. The dichotomy between protection and accessibility/openness arises from the complex nature of public spaces. On one hand, they need to be welcoming and inviting, encouraging people to use and enjoy them. An open and accessible design can foster a sense of community and contribute to social cohesion. On the other hand, there is a need for these spaces to be safe and secure, providing a sense of protection to those who visit them. Ensuring that these dual goals are met can be challenging, as measures taken to enhance security, such as surveillance, barriers, or restricted access, might inadvertently compromise the sense of openness and freedom that these spaces are supposed to provide.

Within the activities of Task 2.3 – Security-by-design approach in urban planning, the SAFE-CITIES project takes a proactive stance in reconciling urban security principles with the concept of adaptive urban planning, all while adhering to the design-for-all principles. The overarching objective of this task is to harmonize security measures with urban planning strategies, ensuring that the safety and well-being of the public are integrated seamlessly into the fabric of the city. Under the design-for-all principles, the project emphasizes that safety and accessibility should be conceived in a way that caters to the diverse needs and expectations of the entire community. This approach encourages the design of public spaces that are not only secure but also welcoming and accommodating for people of all ages, abilities, and backgrounds. This process involves identifying and understanding the overall public space role in urban life including societal, urban planning, design issues, and the physical condition of the public space subject of the assessment.

In particular, concerning the SVA, all information and data collected are used to fully understand what must be protected (targets – step 5), from whom (threats – step 3), and to what performance level (step 6).

SAFE-CITIES project represents a necessary answer to the challenge of balancing both the protection and the accessibility/usability/openness of public spaces. It acknowledges the fact that urban and architectural design of these spaces should be pivotal in determining whether they enhance social safety or they create a vulnerable environment. The dichotomy between protection and accessibility/openness arises from the complex nature of public spaces. On one hand, they need to be welcoming and inviting, encouraging people to use and enjoy them. An open and accessible design can foster a sense of community and contribute to social cohesion. On the other hand, there is a need for these spaces to be safe and secure, providing a sense of protection to those who visit them. Ensuring that these dual goals are met can be challenging, as measures taken to enhance security, such

as surveillance, barriers, or restricted access, might inadvertently compromise the sense of openness and freedom that these spaces are supposed to provide.

Within the activities of Task 2.3 – *Security-by-design approach in urban planning*, the SAFE-CITIES project takes a proactive stance in reconciling urban security principles with the concept of adaptive urban planning, all while adhering to the design-for-all principles. The overarching objective of this task is to harmonize security measures with urban planning strategies, ensuring that the safety and well-being of the public are integrated seamlessly into the fabric of the city. Under the design-for-all principles, the project emphasizes that safety and accessibility should be conceived in a way that caters to the diverse needs and expectations of the entire community. This approach encourages the design of public spaces that are not only secure but also welcoming and accommodating for people of all ages, abilities, and backgrounds. This process involves identifying and understanding the overall public space role in urban life including societal, urban planning, design issues, and the physical condition of the public space subject of the assessment.

In particular, concerning the SVA, all information and data collected are used to fully understand what must be protected (targets – step 5), from whom (threats – step 3), and to what performance level (step 6).

4.1. The concept of public space in the SAFE-CITIES project

Public space has been defined as an environment where strangers come together and meet² forming the backdrop for an intricate web of relationships that evolve, whether intentionally or serendipitously. It is the environment where freedom of movement and expression, on the one hand, and privacy and recollection, on the other, should be guaranteed - the *mise en place* of socio-spatial practices.³ Public spaces serve a myriad of roles in urban life. They are platforms for protest, avenues for participation, stages for performance, outlets for self-expression, havens for relaxation, arenas for activity, and sanctuaries for reflection. These spaces cater to individuals and groups, both indoors and outdoors, playing a central role in shaping the urban landscape and nurturing a pluralistic public sphere. Examples of public spaces span the spectrum of diversity, encompassing tourist sites, transport hubs, shopping malls, places of worship, outdoor markets, concert halls, city squares, parks, streets, pedestrian areas, sporting events, and festivals.⁴

These rights and characteristics offered by public spaces must be guaranteed and stimulated by the urban design of places themselves, to ensure that citizens can continue their daily lives while also enjoying safety and security. However, because of

² Sennett, R. (2020). The public realm. In *Being Urban* (pp. 35-58). Routledge.

³ Lefebvre, H. (1968), *Le droit à la ville*. Anthropos, Paris.

⁴ European Commission (2017). *Action Plan to support the protection of public spaces*. Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions.

this characteristic, all these crowded sites and other 'soft targets' (i.e., shopping centres, open gathering areas and events, non-restricted areas of transport hubs) – whose density may vary during the day or may be temporary⁶ – are the most vulnerable and prone to risks, which need to be dealt with through protection and prevention measures. The challenge lies in the fact that the open and public character of these spaces, which by their nature entail unpredictable actions from the part of their users, make it particularly difficult to adopt protective and preventive measures without altering this nature. It is the intention of SAFE CITIES to integrate counter-terrorism protective security measures with the principles that make public spaces places of relationships: accessible and well connected to other relevant sites, comfortable and inviting (including for safety perception), rich of equipment allowing the performance of a variety of activities, and a sociable environment attractive for different target groups.⁷

These principles are at the core of the place-making approach⁸. Placemaking is a collaborative, community-driven process that seeks to transform ordinary areas into lively, meaningful places where people can gather, socialize, and engage with their surroundings. The placemaking approach considers the physical, cultural, and social elements of a space to make it more attractive and accessible. In this context, considering placemaking as a foundational orientation aims to improve the quality of public spaces by involving citizens in urban planning decisions, supporting health, promoting environmental sustainability and ultimately creating authentic public spaces. This shapes an **integrated approach** that, to be successful, must consider safety as a key factor in urban design, management and programming⁹. Effective, long-term safety measures are counterbalanced with welcoming, well-designed and community-oriented everyday public spaces. In this way, the placemaking approach aligns with the broader goal of creating public spaces that are not only aesthetically pleasing and inviting but also inherently secure, ensuring that residents and visitors can enjoy a sense of safety while participating in community life.

In the context of incorporating safety measures into the placemaking and adaptive planning approach, it is essential to recognize that design interventions must align with a multitude of standards, regulations and requirements. These span several dimensions including 'intangible' aspects – such as preservation and enhancement of historical and heritage value, promoting landscape diversity, fostering nature conservation, maintaining recreational character, accessibility, consolidated uses, walkability, etc. Balancing the public and private interest is another critical aspect to be taken into account. This balance involves accommodating a mix of commercial activities, residential areas and other uses within the public spaces. Moreover, all regulations that

5 European Commission (2022), *Security by Design: Protection of public spaces from terrorist attacks*, p. 94.

6 Home Office of Great Britain (2012, January), *Protecting Crowded Places: Design and Technical Issues*.

7 Friedmann, J. (2010), "Place and place-making in cities: A global perspective", *Planning Theory & Practice*, 11 (2), pp.149-165.

8 Thomas, D. (2016). *Placemaking: An urban design methodology*. Routledge; Madden, K. (2011). *Placemaking in urban design*. In *Companion to urban design* (pp. 654-662). Routledge.

9 Politecnico di Milano, Laboratorio qualità urbana e sicurezza (eds.) (2006-2007), *Pianificazione, disegno urbano, gestione degli spazi per la sicurezza, Manuale, AGIS – Action SAFEPOLIS*.

apply to public spaces must be considered, including those related to mobility, access and transit of emergency vehicles, escape route, requirements for disabled users, fire safety regulations, environmental and cultural heritage legislation; other local urban regulations, etc.).

All these aspects and considerations apply well to public spaces with different characteristics represented by the SAFE CITIES pilots within which the project will test its operational tools.

4.2. Urban design principles for Safe Public Spaces: theoretical framework

The project aims to adopt a 'security by design' approach, a term used to describe "urban design integrating security measures into public spaces and streets without compromising the functions or aesthetics of the space" ¹⁰. This approach emphasizes the importance of proactively incorporating security considerations during the planning and design stages to ensure that safety is an integral part of the space's identity. By adopting this approach, the project aims to create public spaces that are not only secure but also inviting, well-connected, and aesthetically pleasing, promoting the harmonious coexistence of safety and urban liveability. Security-by-design is based on four main key principles describing such an intent:

1. **proportionality:** adequate and balanced security measures with respect to the risk to be faced in order to reduce the impact on daily social and economic activities;
2. **multi-functionality:** safety principles considered (and applied) right from the early stages of design or redesign process, leading to integrated, multifunctional and high aesthetic quality solutions, containing construction costs;
3. **stakeholder cooperation:** holistic cooperation among different stakeholders involved (authorities, architects, planners and police, security specialists, civil society, etc.) is a necessary condition for quality public spaces equipped with effective and properly designed security solutions;
4. **design aesthetics:** solutions embedded into the morphology/design of public spaces capable of combining aesthetics, comfort, usability and functionality in terms of safety without being intrusive or inducing anxiety/fear in civil society.¹¹

The security-by-design approach frames into the 'environmental' prevention line traced by the 'CPTED-Crime Prevention Through Environmental Design' (Jeffrey,

¹⁰ Gehl people, *Basic functions of public space*. Online: <https://gehlpeople.com/blog/basic-functions-of-public-space/>.

¹¹ European Commission (2022), *Security by Design: Protection of public spaces from terrorist attacks*, 2022, pp.23-27.

1971)¹² multi-disciplinary methodology focusing on urban and architectural design, management of built and natural environments. The CPTED acts on all the physical elements present in a certain context to prevent a criminal event from happening, following six main concepts/strategies: territoriality (enhance the sense of appropriation to a specific site); natural surveillance (maximized visibility, social control and interactions); access control (well defined entrance-exit spaces/points); well maintenance and management; activity support (promote functions generating safety perception, e.g., playgrounds); and target hardening (defence of possible specific crime targets).

These concepts advocate the adoption of specific solutions and design strategies aimed at enhancing safety and security within public spaces. Some of these strategies include: display security system signage at access points as both deterrent and reminder of security measures; incorporate multi-modal public transportation; foster pedestrian and cycle routes; install surveillance as closed-circuit cameras; schedule diverse activities to increase vibrancy and liveliness; locate amenities in common areas in order to attract a larger number of users; promote neighbourhoods with mixed population including residents, businesses and visitors; adhere to specific urban lighting design principles; define behavioural rules and clear guidelines for targeted spaces able to incorporate users' safe and respect of their personal and collective rights; use adequate materials and installation rules for urban furniture, without compromising functionality or aesthetics.¹³

Interventions on public spaces embedding safety principles and goals into the design choices should be intended as complementary to other more traditional approaches to urban security, based respectively on the maintenance of public order through the law and the presence reinforcement of the forces of order; and on interventions at social level, aiming at the reduction of conditions of disadvantage and deprivation, considered as a factor increasing the risk of criminal acts.¹⁴ Security-by-design, therefore, can be explored as a right, a social demand, and a policy objective, pursued through a multiplicity of approaches.

In this scenario, urban design and planning, due to its close alignment with public policies, can contribute to the social prevention of risks and unsafe situations when it seeks to shape cities and spaces based on justice, cohesion and sustainability. The aim of this discipline in its integration with security is to “design out”¹⁵ threads for urban public spaces.

Between the exploration of urban design and planning approaches to risk and crime prevention and the alignment of spatial planning with principles such as “design for all,” adaptive planning, and security by design, a key attention on the beauty of

¹² Jeffery, C.R. (1971). *Crime Prevention Through Environmental Design*. Sage Publications, Beverly Hills.

¹³ Perspective.brussels, Department Territorial Strategy (2019, October), *Guide to the integration of security systems in public spaces, Brussels-Capital Region*, pp. 11-13.

¹⁴ Bolici, R., Gambaro, M. (2020), “La sicurezza urbana per la qualità dello spazio pubblico”, *TECHNE* 19, pp. 105-106.

¹⁵ Cozens, P. M. (2011). Urban planning and environmental criminology: Towards a new perspective for safer cities. *Planning practice and research*, 26(4), 481-508.

European cities and their public spaces has come to the forefront.

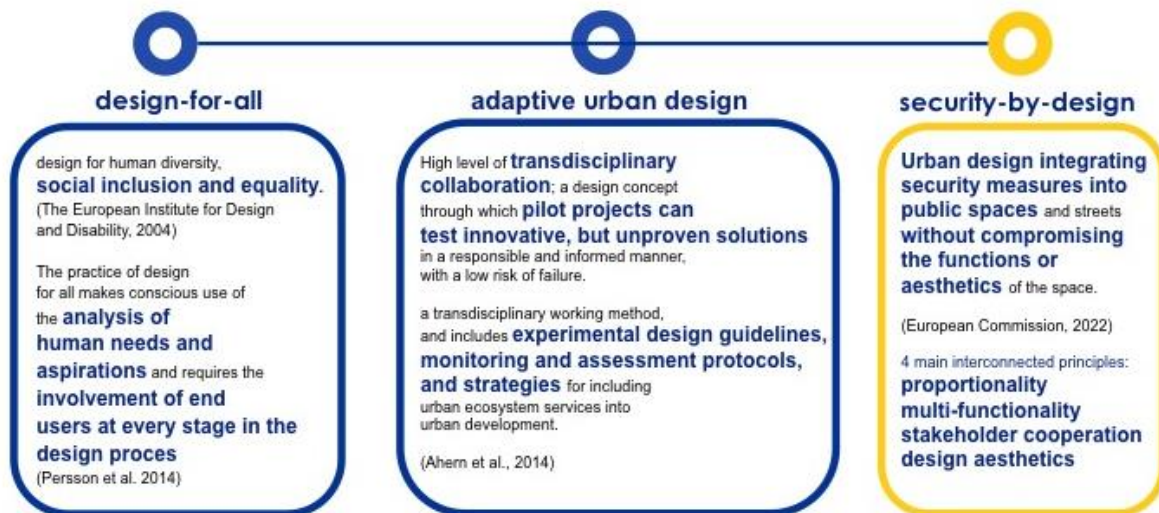


Figure 5: SAFE-CITIES approach to urban design/planning assessment.

A renewed emphasis on the beauty and liveability of EU cities and its public spaces was placed by one of Europe's leading strategies today, the New European Bauhaus (NEB hereon). Introduced by President von der Leyen in 2020, it aims at supporting the EU Green Deal by enhancing cities' capabilities, citizen engagement and behavioural changes. It is grounded in three main pillars, the values of sustainability (climate goals, circularity, zero pollution, and biodiversity), aesthetics (quality beyond functionality), and inclusion (valuing diversity to securing accessibility and affordability). Within the initiative, the focus on public spaces, on their open and co-produced nature, was confirmed by the 2022 call for the "Co-creation of public spaces"¹⁶ in support of citizen-led initiatives, launched within the NEB framework by the European Institute of Innovation and Technology (EIT). During its co-design phase, the NEB asked the involved stakeholders to identify the challenges to the implementation of beautiful, sustainable, inclusive places, and safety occupied a prominent and central place. Similarly, in the recent European Urban Initiative call, the regeneration of urban spaces was epitomized as the provision of "universal access to safe, open, and inclusive green and/or public spaces".¹⁷

Therefore, what emerges in the NEB framework is the tight coupling of safety and inclusiveness of public spaces, as both a challenge and an imperative which should be pursued to create liveable and beautiful cities. For this reason, counter-terrorist safety and security measures should consider and be tailored to the peculiar features and nature of public spaces subject to risks and, therefore, incorporate a combination of approaches, strategies and measures, (if applicable) from the very onset of the

¹⁶ https://new-european-bauhaus.europa.eu/about/co-design-process-and-contributions/overview-challenges_en

¹⁷ <https://www.urban-initiative.eu/new-european-bauhaus-topic-first-call>

planning and design process in order to be better integrated within the surrounding built or natural environment, while also looking at how the main beneficiaries of those spaces, i.e. citizens, should be incorporated in the planning and design of these measures as well as in the co-creation of public spaces.

It goes beyond the scope of the present research to discuss all the different methodologies of co-creation and co-design for public spaces in cities; what will be presented in this section is a "Survey On Citizens' Awareness and Perceptions about Security in Public Spaces" to analyse citizens' perceptions about the security of public spaces, designed within SAFE-CITIES in T2.2 ("Citizen participation") and applied to the four use cases of the project. Embracing the design-for-all perspective, the survey supports planners' ability to 1) understand human desires and aspirations with respect to the potentialities and values attached to urban public spaces; 2) identify risk perceptions related to attending events in open / closed public spaces; 3) understand the social and cultural relevance of a given public space, not only to quantify the attractiveness to potential threats but also to assess the degree to which the landscape of that space can be altered by physical interventions. The results of the survey - still in the processing phase - jointly with empirical evidence emerging from the engagement activities with the Local Citizens Networks (Task 2.2), may provide further inputs to the SAFECITIES project.

This work supports urban planners and designers in the implementation of safety and security measures which hinder, rather than elicit, the perception of threats from the part of citizens. It aims to prevent an undue sensitivity to risk, which could otherwise result in an overabundance of physical barriers, control measures, and an increased police presence. Instead, it encourages the adoption of a security-by-design approach in public spaces, aligning to the European Commission's intention, expressed by NEB, to create inclusive, resilient and beautiful public spaces.

All these inputs converge in the theoretical framework of the SAFE-CITIES approach to urban design, defined by working on three main strands:

1. The definitions of **a set of urban design principles for safe public spaces**, integrating the design approaches mentioned above (design for all, adaptive design, the NEB values and the main principles of security-by-design, as reported by the European Commission), thus, combining general aspects - such as the importance of avoiding oversensitivity to risk, assessing the value of places, etc., and more operational actions - for example related to the design or layout of the furnishings, as well as hybrid solutions between urban art, and environmentally sustainable actions.
2. The **collection of case studies**, and best practices, mainly consisting of open spaces, either built or partially built having public ownership and/or use, integrating different protection measures (e.g., bollards, topography, benches, trees and greenery, vegetable pots, pavilions, etc.) also including temporary solutions, providing useful insights on the balance between openness and risk prevention in public spaces.

3. A **literature review**, supporting the definition of a scientific bases for the research, from which two main integrated approaches emerge: the first linked to more general planning strategies, also dealing with more 'intangible' factors (e.g., accessibility, functional mix, natural surveillance, stakeholder engagement, etc.); the second concerning the application of operational design measures (e.g., furnishings, topography, materials, etc.), standards and regulations.

Such a knowledge base – preliminarily reported in Deliverable D2.1 - represents the theoretical background for the development of a general methodology which resulted in a tool named 'Atlas 4 safe public spaces design-guiding framework' supporting the virtual testing of the security-by-design approach/principles on the pilots and incorporating Local Citizens Networks' (LCN) feedback.

4.3. 'Atlas – 4 safe public spaces design guiding framework'

The 'Atlas 4 safe public spaces design-guiding framework' is an operational tool supporting the evaluation of some socio-technical aspects and features of the urban space which might not be considered in traditional security assessment tools.

The Atlas – proposed as annex to the SAFE-CITIES SVA – might work as a 'compass' for security-by-design-led interventions. The Atlas is inspired by the NEB methodology known as "NEB compass",¹⁸ a methodological tool developed for guiding decision and project makers in operationalizing the values of NEB (beautiful, sustainable, together) through a set of working principles (participatory process, multi-Level engagement, transdisciplinary approach) to their activities. The working principles all have different degrees of application, the so-called "ambitions", whose intensity depend on which working principle is pivotal in the project (as an example, in the case of "participatory process, the three levels of implementation are "to consult", "to co-develop" and to "self-govern"). Projects examples complete the compass, providing some guiding questions for assessing and supporting the Compass' application.

While the NEB represents one of the core pivots of the security-by-design approach in the SVA of SAFE-CITIES, it is not the sole policy reference; NEB is an overarching inspiration and strategic approach, and the NEB compass served to articulate the Atlas described below, while other major policy documents such as the 2022 document of the European Commission on "Security-by-design: protection of public spaces from terrorist attacks" and the 2017 EC "Action plan to support the protection of public spaces". These and other documents were pivotal in articulating the recommendations and guiding questions of the Atlas, as illustrated in the methodological articulation of the tool which follows.

¹⁸ The New European Bauhaus compass, https://new-european-bauhaus.europa.eu/get-involved/use-compass_en.

The Atlas is organized as a matrix/table working as follows:

1. It starts from three main '**levels of attention**' to be considered in assessing the design of urban spaces in terms of safety, inclusiveness, beauty and sustainability, which embrace in clusters the principles previously defined: these are the methodological approach, i.e. the underlying approach to the intervention, the users' engagement, i.e. the level of interaction with the relevant stakeholders and the phase in which their contribution would be incorporated; and physical interventions, meaning the urban furniture and physical objects which would be placed in space.

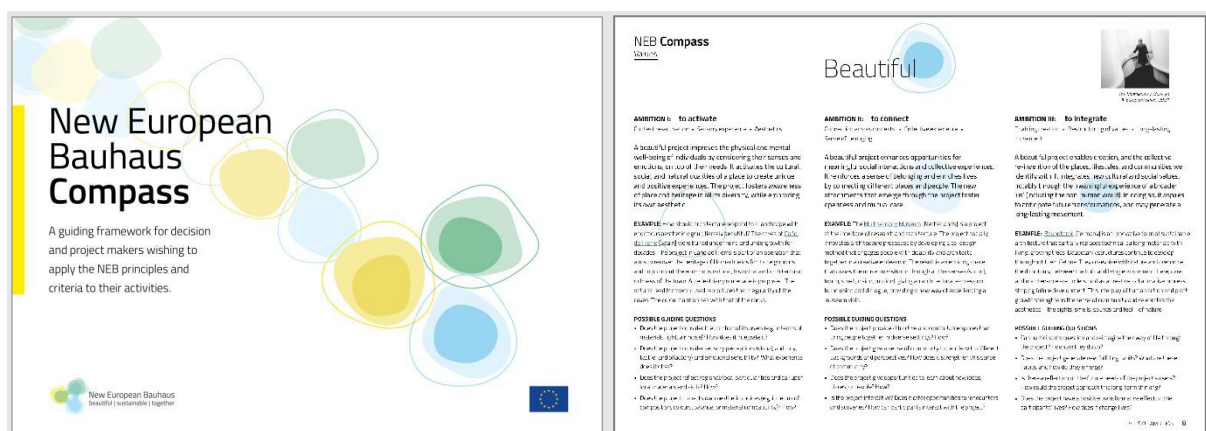


Figure 6: The NEB Compass – extract (<https://new-european-bauhaus.europa.eu/get-involved/use-compass-en>).

2. Each level is broken down into clusters of transversal **ambitions**, i.e., the goal/s to be reached for each different level of attention. The ambitions, in particular, draw from the EU priorities and recommendations, as identified in all the relevant policy documents; where deemed necessary, other sources concerning the security-by-design approach were taken into account.
3. Each ambition is then associated with a set of **recommendations**, which operationalize the EU recommendations and the ambitions of the present methodology; similarly to ambitions, recommendations were inspired by policy documents and relevant reports and studies on security-by-design.
4. **guiding questions** clarify the recommendations and prove helpful for several dimensions of the SVA, especially those concerning the quantification of the attractiveness and relevance of the space (Step 5).
5. **Insights from case studies** for each level of attention/ambition (useful design examples to understand how to achieve ambition/s) conclude the Atlas. In particular, the design examples collected will define as additional output a portfolio of projects, initiatives and experiences from which to draw inspiration and lessons learned. The cases were selected so as to feature a wide variety of European (and non-European) contexts, diverse urban conformations and typologies of space, in order to illustrate the versatility of the tool.

6. The bottom row includes **references** (including documents, papers, policies, regulations, etc. defining the scientific basis); these references were, in particular, those inspiring the ambitions and recommendations, to reconnect the SVA to the broader policy ecosystem concerning the security of public spaces in Europe and to the New European Bauhaus.

Below, the main contents of the Atlas in terms of ambitions, recommendations and guiding questions - organized under the three defined levels of attention - are listed, while the complete Atlas (A3 printable format board) and the portfolio of design examples (A4 Format) are available as Annexes 3 and 4.

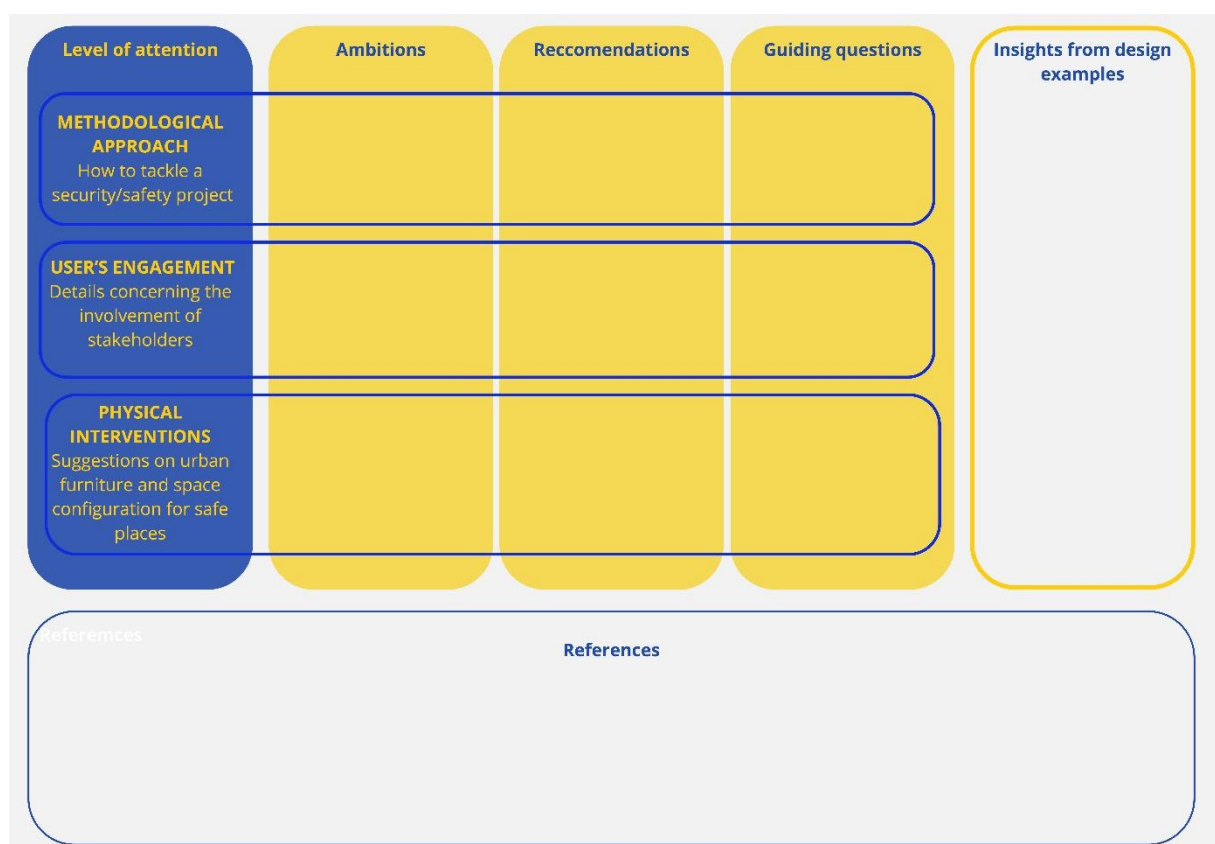


Figure 7: 'Atlas – 4 safe public spaces design guiding framework' structure.

1. METHODOLOGICAL APPROACH: how to tackle a security/safety project

Ambition 1.1: Avoid oversensitivity to risk

- *Recommendation/s:* Ensure proportionality between measures and potential risks¹⁹; Ensure balance between safety/protection and open nature of public

¹⁹ Home office of Great Britain (2014). *Protecting crowded places: design and technical issues*.

areas/openness.²⁰

- *Possible guiding questions:* Does the design facilitate natural surveillance, allowing people to observe and have a clear perception of the space?

Ambition 1.2: Consider security measures from the early stage of design process

- *Recommendation/s:* Avoid relying solely on barrier-based solutions; instead, integrate security measures with a broad vision of 'beautiful, sustainable and inclusive' public spaces, in line with the New European Bauhaus principles.²¹
- *Possible guiding questions:* Have the security needs and expectations of the public space's users been considered and incorporated into the design process from an early stage?

Ambition 1.3: Integrate existing policies

- *Recommendations:* Testing/assessing the application of existing policies specifically tailored for accessibility of spaces, inclusion of vulnerable categories through surveillance, preventive design for safe spaces.²²
- *Possible guiding questions:* Are safety and security measures designed in compliance with design-for-all principles?

2. USER'S ENGAGEMENT: details concerning the involvement of stakeholders

Ambition 2.1: Sharing processes of safety design

- *Recommendation/s:* Create shared informed decisions-making processes following more collaborative and inclusive processes among a wider as possible stakeholder group²³; Maintain an open and transparent process of monitoring and developing of safe spaces.
- *Possible guiding questions:* How do you engage with stakeholders to understand their risk expectations and tolerance? How do you foster continuous improvement of risk assessment and management within your city?

Ambition 2.2: Intersectional approach: incorporate vulnerabilities and differences.

- *Recommendation/s:* Consider different mobility impairments into the approach; Consider generational and gender approach in security by design; Incorporate needs, behaviours and responses of different citizen's types²⁴ into the simulations

²⁰ Nadel, B. A. (2004), *Building security: Handbook for architectural planning and design*. McGraw Hill Professional, New York.

²¹ European Commission (2022), *Security by Design: Protection of public spaces from terrorist attacks*, 2022, p.26.

• ²² United Nations Office of counter-terrorism (2022), *Protecting urban centres from terrorist attacks – Good practices guide*, Module 2, Global Programme on Countering Terrorist Threats against Vulnerable Targets.

²³ European Commission (2022), *Security by Design: Protection of public spaces from terrorist attacks*, 2022, p.26.

²⁴ Gehl - Making Cities for People (2022), *Public Space and Public Life during COVID-19*.

of threat scenario.

- *Possible guiding questions:* Are you communicating effectively about risk to stakeholders, ensuring they have a realistic view of potential outcomes? How are different community voices been incorporated in the design of safety measures?

3. PHYSICAL INTERVENTIONS: suggestions and recommendations on urban furniture and space configuration for safe places.

Ambition 3.1: Combine and integrate protection systems with a physical design of the space/area.

- *Recommendation/s:* Display the creation of barriers and boundaries protection systems according to the existing layout/asset of the space/area in order to prevent risks and threats; 25 Respect and complain with the function, social and symbolic value of space (e.g., UNESCO sites).
- *Possible guiding questions:* Do the protection systems take into consideration the urban and architectural layout of the space? Do barriers or other safety devices ensure the smooth running of activities in the space?

Both temporary/exceptional/seasonal (e.g., market, etc.) and daily/conventional (e.g., walking, staying, entrances, accesses, fluxes, etc.)?

Ambition 3.2: Ensure the integration/balance between standardized and ad-hoc protective measures.

- *Recommendation/s:* Combine certified/ standardized urban furniture for security response (e.g., benches, bollards, natural barriers, rails and fences) with other 'environmental' solutions (e.g., territoriality, natural surveillance, access control, well maintenance and management, and target hardening), as well as ad-hoc protective measures (e.g., public art). 26
- *Possible guiding questions:* Are the protection systems adopted all of the same type or do they integrate multiple solutions?

Ambition 3.3: Consider measures enabling multifunctional uses (beyond just the security functionality).

- *Recommendation/s:* Prefer urban furniture/ systems/solutions capable of enabling multiple uses; Check if the urban furniture/ systems/solutions are compatible with the daily usability and comfort of the space (e.g., sunny and shaded areas).
- *Possible guiding questions:* Are the activities that usually take place in the space guaranteed by the solutions adopted? Do the planned urban furniture/elements serve multiple purposes? (e.g., the bollards that protect the space organize areas

25 Perspective.brussels, Department Territorial Strategy (2019, October), *Guide to the integration of security systems in public spaces*, Brussels-Capital Region, p.27.

26 Perspective.brussels, Department Territorial Strategy (2019, October), *Guide to the integration of security systems in public spaces*, Brussels-Capital Region, pp. 19-34.

for different uses; the barriers are useful as noticeboards or as signs, etc.).

Ambition 3.4: Consider the climate and environmental mitigation purpose/aspects in the design layout

- *Recommendation/s:* Provide protective measures/solutions serving as climate and environmental mitigations solution (e.g., plants, tree-lined streets, hills, water retention devices, etc.).²⁷
- *Possible guiding questions:* Have you performed an environmental assessment of the site to identify possible vulnerabilities? Does the project have a positive contribution in terms of improving the outdoor comfort of the space?

Ambition 3.5: Combine different types of security systems capable of responding to different emergencies/attacks.

- *Recommendation/s:* Ensure the insertion of physical measures in the streetscape for specific attacks (e.g., vehicles); Apply when possible general planning principles: turn areas into pedestrian routes, keep attention to access points and boundaries, identify sensitive points, identify targeted routes and access points (e.g., logistic, emergency vehicles, concentrating vehicle flows by defining protected areas, etc.); Integrate specific systems into the public space hosting public services/uses and at the same time providing/defining obstacles (e.g., furniture, topography, pavilions, etc.); Ensure integrative mechanical surveillance measure (CCTV); Test the planned solutions with temporary experimentations.²⁸
- *Possible guiding questions:* Have you considered existing urban furniture when implementing safety measures? Have multiple and differentiated safety systems been adopted?

The Atlas - working in synergy and implementing the SVA - is intended to support end-users, designers, decision and policy-makers in the assessment of the SAFE-CITIES security-by-design approach in design proposals/interventions, temporary installations, public events, etc.

²⁷ European Commission (2022), *Security by Design: Protection of public spaces from terrorist attacks*, 2022, p. 34.

²⁸ Ibidem.

5. The role of public – private partnerships the public space protection

Today there are two million private security officers in Europe – a number comparable to police officers. Private security companies (PSCs) are present in every citizen's life: they conduct controls at airports and concert halls, secure Critical Infrastructure, and protect public spaces such as shopping malls, sports and leisure venues, festivals, and other private property.

The widening footprint of services provided by PSCs, which in public spaces has evolved at a different pace in various Member States, has become a reality. The rise in terrorist threats in Europe during the past decades, but also other socio-economic developments such as the COVID-19 pandemic, have intensified the realisation that the PSCs cannot only deliver innovative security solutions to uphold public safety and security, but also offer a potential of additional eyes and ears, when adequately informed and trained, and therefore reinforce the prevention and detection capability of Law Enforcement Agencies (LEA) – if organised in a public-private collaboration.

Such public-private collaboration, also known as “The Security Continuum” can take place in various forms, starting from an exchange of contact points and going as far as security and vulnerability assessments (SVAs) for the protection of public spaces and joint trainings. It is the condition for an effective global security framework that fully plays its protecting and preventing role, and that all players can therefore trust and rely upon.

Public-private collaboration between LEAs and PSCs should however be built on a number of general rules and follow certain principles and values in order to build trust. As the results of this project show, the potential of public-private collaboration, particularly in the form of joint SVAs, is not yet implemented in a large number of European countries.

This chapter will therefore look into:

- the legally defined competencies and tasks of PSCs for the protection of public spaces,
- the extent of existing public-private collaboration between PSCs and LEAs in European countries,
- existing frameworks, including what kinds of collaboration they include,
- the organisation of public-private collaboration and whether it's formal or rather informal.

Finally, this chapter provides recommendations and guidelines on how to establish public-private collaboration, and steps to intensify such frameworks particularly in the form of joint SVAs.

5.1. The European Commission's Good Practices to support the Protection of Public Spaces” and Recommendations for public-private collaboration

An important baseline for public-private collaboration in the protection of public spaces is the European Commission Staff Working Document 2019/140 on “*Good practices to support the protection of public spaces*”, which was developed jointly by the Commission, Member State authorities, operators of public spaces, and the Confederation of European Security Services (CoESS). Regarding public-private collaboration, important good practices include:

- **Security culture:** Develop of a common culture of security, shared between public authorities, private actors, and citizens.
- **Vulnerability and Risk Assessments:**
 - Regular vulnerability assessments to be conducted in a public-private collaboration approach, followed by tailor-made security measures.
 - Public authorities should share risk assessments and information as appropriate, and a trustful and timely communication and cooperation that allows for a specific risk and threat information exchange between responsible public authorities, local law enforcement and the private sector should be established.
- **Clear roles, responsibilities and communication:**
 - Public and private operators should appoint a competent person, as well as a backup, who understands the threats landscape and knows well the facility/event and make sure that this person receives the appropriate training.
 - Every actor involved in the security chain should appoint contact points and clarify respective roles and responsibilities in public-private cooperation on security matters (e.g. between operators, private security and law enforcement authorities) and for a better communication and cooperation on a regular basis.
 - Operators shall ensure efficient management and communication in crisis situations with staff and customers, as well as with law enforcement, with the help of technology, crisis communications teams and clear messaging.

- **Training:**
 - Staff working at the facility or event should be properly trained and regularly re-trained for the tools they operate. In addition to the Commission document, CoESS recommends that appropriate training and qualification of critical personnel is also to be checked in procurement practices, if the performance of security measures is outsourced, as recently recommended by the EU Directive on the Resilience of Critical Entities.
 - Undertake regular security exercises that will help to identify the level of preparedness to deter and respond to an attack, involving all relevant stakeholders (e.g. rescue services, special forces and other relevant service providers).
- **Physical protection:** Public and private entities need to be involved to better take into account protection issues in the design of buildings and other spaces.
- **Insider Threats:** Based on the vulnerability assessment, and in close cooperation with law enforcement authorities, operators of public spaces should consider background checks and possible vetting of the staff in respect of national laws both before and during their assignments. The EU-funded AITRAP project (www.help2protect.info) which was coordinated by CoESS, provides an Insider Threat online training programme and is a good example for such a tool.

5.2. Views of the European private security services industry: state of play of public-private collaboration for the protection of public spaces

As part of the SAFE-CITIES project, CoESS conducted different surveys on public-private collaboration for the protection of public spaces, both among national associations and private security companies, in 30 European countries. These surveys were complemented by additional desktop research and outreach, and cover all EU Member States, except for Austria and Cyprus, as well as the following non-EU Member States:

- North Macedonia
- Norway
- Serbia
- Switzerland
- Turkey
- United Kingdom (UK)

The research focused as a baseline on the implementation of the European Commission's Good Practices document, but went also further and looked into currently existing models of public-private collaboration for the protection of public spaces, and particularly the extent to which joint SVA's are already a reality – including respective success factors to take into account in the SVA framework.

5.2.1. The precondition: national regulation on private security tasks and competencies in public spaces

Whether or not private security companies are allowed to conduct missions on behalf of, and/or in cooperation with, law enforcement authorities (LEA) to complement activities for the protection of publicly accessible spaces – both public (such as streets, public festivities, asylum centres, etc.) or private (such as transport networks, stadiums, privately operated festivals, etc.) perimeters, depends on the regulation of the sector at national level. But only in roughly half of the countries covered by this research, PSCs are allowed to provide such services.

There is however an important difference in regulation between European regions:

- In almost all North and West European countries, PSCs can provide services in support of or on behalf of LEA for the protection of public spaces. In some countries, like Sweden and the UK, legislation is quite detailed and even requires that companies and/or security officers have a specific license, in addition to the legally obligatory / basic one, to conduct missions on behalf of, and/or in cooperation with LEA in public spaces.
- In contrast, PSCs do not provide such services in most East and Southeast European countries (except for Croatia, North Macedonia, Serbia and Turkey).

It also depends on national legislation in which public spaces PSCs are allowed to conduct missions. Where they are allowed to provide such services, this usually includes public events as well as sports and festival facilities. Other public spaces covered include transport networks, hospitals, asylum centres, public administration facilities, and recreation facilities such as parks or beaches.

Tasks and competencies of private security officers protecting public spaces are likewise subject to national legislation. When private security officers conduct missions in public spaces, these are always purely preventive tasks and usually include:

- Access control
- Monitoring and remote surveillance
- Patrolling and perimeter control

In some countries, these also include the public retention and/or detention of criminal offenders until law enforcement arrives.

5.2.2. Added value of private security in the protection of public spaces

Deploying private security services in public spaces is not a question of simple outsourcing, but complementarity and pragmatic solutions to work towards the highest possible level of public security. This is echoed by the research conducted as part of the SAFE-CITIES project. Reasons to engage PSCs in the protection of public spaces, as per the framework and remits set by national law, include:

- **Human resources:** Private security can free up LEA resources, so they can focus on complex tasks for which they have the equipment, training and special rights – for example in counterterrorism. If preventive and protective tasks can be taken over by private security under respective regulation and strict public oversight of activities, it is a choice of the State to decide whether they will be. Public forces do not lose control of public security because tasks are delegated. Oversight of private security activities should be well defined in contracts and reporting procedures – and frameworks for public-private collaboration.
- **Enhanced security:** Private security can offer different skills and eyes to be an effective addition to LEA. Security companies have a different mindset and therefore can give a different perspective and output to LEA that they otherwise would not have. It also enables both parties to focus on their core skills and competencies. Within the criminal planning cycle, PSCs are also the organisations that are focusing on the first steps of prevention and detection, before the incident occurs. PSCs can prevent criminal actions and, if needed, assist government agencies in fact finding / providing information.
- **Specialisation of PSCs:** For example, in airports, the screening of passengers and baggage has become a very specialised job, which does not need to be performed by LEAs. Also, the professional security market has four times more operators than LEAs. Companies can often respond quicker to urgent demand and can offer some specialist skills through dedicated companies. It is important to recognise that private security has decades of experience in securing assets such as Critical Infrastructure, special events and (semi-) public spaces, and brings special capacities and capabilities to the table.
- **Innovation:** Companies constantly invest in the future, including training of personnel and use of state-of-the-art technologies in order to propose the best and most appropriate security solutions. They constantly assess emerging risks to enhance resilience within an evolving threat environment. LEAs do not have constant pressure from clients and they do not have competitors, and are therefore not as close and responsive to the market needs as PSCs. At the same time, technology provides additional opportunities for better coordination and cooperation among public and private forces – for example, when it comes to

providing access to video surveillance images to LEA. But in the concept of the “New Security Company”, PSCs also increasingly follow the integrated security approach by bringing people, technology, and processes together through investment in the connected officer.

- **Flexibility:** PSCs bring flexibility and agility related to human resource capacity and operations. Their quality management and measurement are stronger due to clear KPI's in the contractual relationship with LEA.

5.3. Framework for public-private collaboration and Joint SVAs

Although recommended by the European Commission's Good Practices document, formal frameworks that organise public-private collaboration could only be identified in 11 out of 30 countries. Where they exist, they are in large majority established at municipality-level (77%), but also at regional and national level (both 55%). In 80% of the cases, these collaboration frameworks are of permanent nature and not only temporary. These frameworks are rarely set out in legislation, except in countries such as Sweden and Switzerland.

When formally organised, public-private collaboration frameworks reflect important recommendations made by the European Commission, such as:

- Establishment of respective points of contacts among LEA, PSCs, and other local actors (75%)
- Regular formal forums of information exchange at management level, e.g. roundtable or Committees (65%)
- Live information/data exchange in case of suspicious behaviour or an incident between PSCs and LEA (55%)

It is also important to note that, in 60% of the cases, PSCs are first subject to selection criteria before participating in this cooperation – a key recommendation of the private security industry made later in this chapter.

Other means of collaboration, which are also part of the European Commission's Good Practices, include:

- Jointly increasing security awareness among the public (40%)
- Joint trainings with the operator of the publicly accessible space (35%)

LEA and PSC resources are only pooled in 30% of the cases. However, those collaboration approaches which are in the focus of the SAFE-CITIES project, joint risk and vulnerability assessments and joint trainings with LEA, are the least means of collaboration reported by companies themselves:

- 19 out of 29 security companies interviewed as part of the survey indicate that they conduct missions on behalf and/or in cooperation with LEA for the protection of public spaces.
- In 72% of the cases, these missions are accompanied by frameworks of public-private collaboration mostly including means of collaboration mentioned above.
- However, only five companies responded that they are or have been formally invited to also conduct joint risk and vulnerability assessments in collaboration with LEA and/or operators of the public space,
- Only three companies conduct joint trainings with LEA.

Despite these low numbers, we asked all participating companies separately on requirements to conduct joint risk and vulnerability assessments with LEA, which reflect these results. Notably, they witness that LEA are often reluctant to involve private partners in the preparation phase of a security plan. PSCs are too often seen as a late entry enforcement tool. This is why the industry still has to pro-actively make its voice heard and call for formal measures that can build more trust.

We have further asked both PSCs and national industry associations how that trust can be built concretely. An important recommendation in this regard is (1) the establishment of quality criteria for the selection of security services protecting public spaces, by legislation or for example (2) with the help of Standards and Norms:

1. An important point mentioned are selection criteria to be used when procuring private security companies for the protection of public spaces. Tender processes should not only focus on the costs of the services provided, but also make sure that the security company can demonstrate that it has the adequate capabilities and experience / quality in establishing security concepts for the protection of public spaces. Establishing such selection criteria would be a first important stepping stone for building trust and joining forces in a public-private collaboration, particularly with a view to joint SVAs and data exchange.
2. A very useful selection and hence quality criteria can be the compliance of security companies with specific International and/ or European Standards. PSCs surveyed as part of this research use a wide range of certifications to prove adequate qualification and quality of specific business solutions to build trust for enhanced information exchange and collaboration with LEAs, for example:
 - a. EN 17483 - Private Security Services – Critical Infrastructure Protection
 - b. EN 50518 – Monitoring and Alarm Receiving Centres
 - c. ISO 27000 – Information Technology

- d. ISO 22300 – Security and Resilience
- e. ISO 31000 – Risk Assessment
- f. ISO 28000 – Supply Chain Security
- g. ISO 9001 - Quality Management
- h. Other national Standards and Norms – e.g. The Nederlandse Veiligheidsbranche (Dutch Private Security Association) has developed various quality marks, under the heading of “Keurmerk Beveiliging” (security quality mark). Security activities can be subdivided according to the various forms of security services within the industry. The activities, and the rules a company must comply with, differ from one another. The Keurmerk Beveiliging recognises these differences, which is why a set of six quality marks have been developed.

5.4. Recommendations and guidelines of the private security industry for enhanced public-private collaboration

This research shows that the baseline requirement for public-private collaboration is legislation and formal frameworks. CoESS has been seeking for many years to raise the legislators' awareness to the need to step up the quality and compliance with standards for private security in general, but even more so for those PSCs that protect public spaces and engage into public-private collaboration. This will build trust, which will be essential for a well-functioning, formal, framework of public-private collaboration, including joint SVAs and trainings.

As part of this research, also PSCs provided recommendations and guidelines on how to improve public-private collaboration in Europe – which reflect CoESS' demands and which are ranked below by level of priority, as follows:

1. Trust, and hence selection of qualitative security service providers.
2. A legal basis and/or formal frameworks for public-private collaboration.
3. Clear definitions of roles and responsibilities.
4. Clear frameworks for information exchange.
5. Regular evaluation of the public-private collaboration framework.
6. Possibility to pool resources in terms of personnel and technologies.
7. Data interoperability.
8. Safe and cybersecure channels for live exchange of data in case of an incident.

Apart from this legal baseline, we have grouped the success criteria and respective recommendations of participants in our research in three clear steps to follow, for the establishment of public-private collaboration, which can include joint SVAs and trainings:

Step 1: Ensure the selection of qualitative services

- Public and private procurers should make sure that the call abides by (1) the laws and obligations to PSCs, to (2) the Most Economically Advantageous Tender (MEAT) principle, as well as by (3) collective agreements and (4) any relevant standards.
- A valuable help can be the establishment of selection criteria for companies participating in this cooperation. Such licenses can be set by law, such as in Sweden and the UK, or industry-led, like in the Netherlands.

Step 2: Set up comprehensive public-private collaboration frameworks

- Determine the scope of the cooperation, clear operational and measurable objectives, and each party's commitment to reach them.
- Description of roles, responsibilities/liabilities and missions of each party and clarify expectations for the LEA, the PSC and the Client.
- Determine the procedures and routines for the operational cooperation.
- Determine the procedures for the exchange of information (timing, format, contact points), clarify data operability and establish levels of classified information that can/needs to be exchanged.
- Determine the contact points and meetings where LEAs and PSCs can exchange information and experience, as well as give any necessary feedback.
- Set up regular meetings, attended by participants at managerial level and with the competences relevant to the agenda (permanent members and ad hoc members).
- Agree on formats and procedures for the meetings and give space to feedback and improvement.

Step 3: Promote and implement security awareness, culture and training programmes as part of the public-private collaboration

- The parties should identify and meet the needs for security awareness, culture and training with the environment covered by the collaboration framework, depending on the targeted audience.
- Security awareness: the general public should be encouraged to report any suspicious behaviour or activity to a central contact point.

- Security culture: the staff working in the environment should be sensitised to security issues and understand how they are part of the chain and can help detect and prevent incidents, including with Insider Threats.
- Security training: this should be provided for specific groups of security or security-related staff, but also joint trainings with LEA and the operator are strongly recommended, as mentioned in the European Commission's Good Practices document.
- Security plans: This can include joint SVAs, the possibility to pool resources in terms of personnel and technologies, and the establishment of safe and secure live information/data exchange in case of suspicious behaviour or an incident between PSCs and LEA.

6. The SAFE-CITIES SCPM within SVA

6.1. Introduction

The SAFE-CITIES Participatory Model (SCPM)²⁹ is a comprehensive methodological framework designed to engage citizens and stakeholders in local processes aimed at enhancing vulnerability analysis for public space security and related planning at the local level. The SCPM offers a standardised approach through which practitioners, managers, and decision-makers can establish local informal partnerships with representative stakeholders and develop targeted engagement strategies to support the preparation and implementation of Security and Vulnerability Analysis (SVA) exercises.

The SCPM is structured into three main operational phases:

Phase 1 – Assessment

Phase 1 focuses on analysing the features and key actors within a specific context, considering the Security Ecosystem at stake. This phase consists of two assessment steps: Community assessment and Stakeholder assessment, which gather information for contextualising the SCPM within a specific Pilot Site. Phase 1 is executed by T2.2 coordinators (ISIG) in collaboration with WP2 partners through data collection activities, including surveys, focus groups, and secondary data analysis.

Phase 2 – Contextualisation

Phase 2 interprets the results of Phase 1 data analysis to adapt the SCPM for the specific context/Pilot Site. This phase involves "Sense-making" workshops facilitated by ISIG and local partners, leading to the formation of the Local Citizens Network (LCN) and the development of the Stakeholders' Engagement Strategy (SES).

Phase 3 – Implementation

Phase 3 encompasses the actual implementation of SAFE-CITIES engagement activities, primarily driven by partners at Pilot Sites. It includes launching LCN activities, executing the SES, and conducting monitoring and evaluation actions to assess the outcomes achieved through LCN activities and SES implementation.

6.2. Local Citizens Networks (LCNs)

Local Citizens Networks (LCNs) are voluntary partnerships comprising civil society and security stakeholders in SAFE-CITIES Pilot Site communities. They are established based

²⁹ The model methodological approach and operational steps are detailed within the D2.1 -SAFE-CITIES Participatory Model – version1.

on a standardised stakeholder mapping methodology, led by Pilot Site coordinators/partners with support from Task 2.2 coordinators during SCPM Phase 1.

6.2.1. LCN Structure

Each LCN is ideally structured into three tiers:

- First tier – Partnership circle: Comprising core team members who are highly knowledgeable and interested in engaging in strong cooperation for SAFE-CITIES activities and local security planning processes.
- Second tier – Communication circle: Comprising stakeholders with either high knowledge/capacity or high interest toward the exercise at hand. Activated for specific steps/topics relevant to the SVA exercise.
- Third tier – Information circle: Comprising stakeholders with low levels of both relevance and interest, primarily focused on ensuring transparency and openness of the SVA exercise to the community.

6.2.2. Engagement Strategies

LCNs are expected to contribute to various project activities, including SVA, validation, and awareness raising. The aim is to strengthen a culture of safety and security in public spaces, ensuring that SAFE-CITIES solutions are embraced by both security stakeholders and civil society. The SCPM enables a co-production approach, fostering structured dialogue between security actors and local stakeholders and citizens. Action Plans for engagement are developed based on the specific context and the outcomes of Phase 1 and Phase 2 of the operational framework, providing operational steps and tools for partners and LCNs, as well as monitoring and evaluation tools.

7. The SAFE-CITIES SVA

Chapter 7 introduces the final version of the SVA steps as finally derived from the iterative process identified previously in Section 2.2. Within the present document and in order to avoid replicating D2.1, *it was decided to include the most important methodological points that needs to be considered by a potential organization that will attempt to implement the SVA*, in order to avoid going back and forth between this document and D2.1. Appropriate references and links to the document are made.

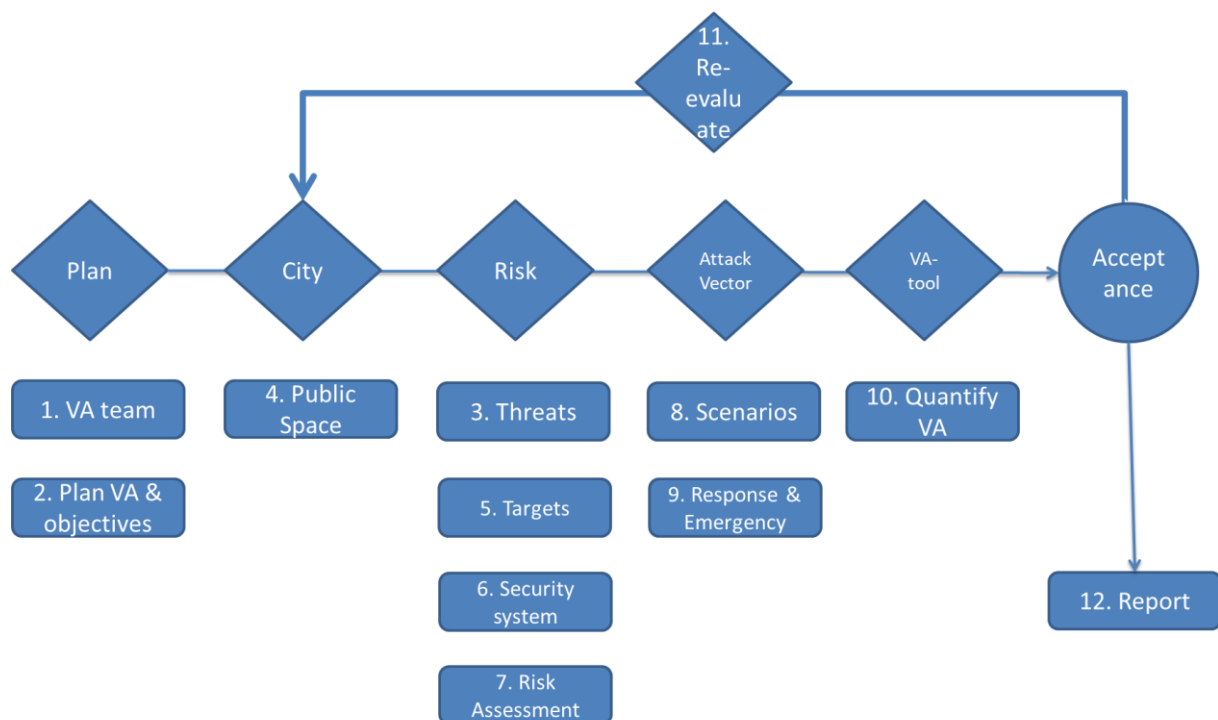


Figure 8: Final version of the SVA 12-step process.

7.1. Step 1. Identify the SVA Team

Each public space protection project is unique and will require the establishment of an integrated team of diverse expertise that matches the goals of the project. The team should be assigned **a project lead (or lead team)** that can manage the entire SVA process and ensure the assessment and results are properly validated, aligned with national and/or local practices and easily comprehensible by security personnel. Table 3 introduces a descriptive analysis of potential roles and responsibilities that can be included in the SVA team.

Table 3: SVA Team roles and responsibilities.

Roles	Responsibilities
Project Manager (or managing team)	<p>Selects administrative and security professionals with sufficient expertise.</p> <p>Sets realistic schedules and budgets (when appropriate).</p> <p>Sets holistic vision and orchestrates team.</p> <p>Day to day management and reporting</p>
Public Space (or Event Managers)	<p>Support a long-term development strategy and comprehensive site design.</p> <p>Support long-term management.</p> <p>Integrates public space role in daily urban life</p> <p>Share expertise on the detailed operation and everyday functionality of the building and site.</p> <p>Establish relationships with stakeholders.</p>
Municipalities / Local Authorities	<p>Budget and funding issues</p> <p>Support multifaceted, holistic strategies linked to local/national policies.</p> <p>Identify acceptable risk levels</p>
Security Experts	<p>Set security and emergency response plans, conduct VA</p> <p>Setup physical protection and countermeasures.</p> <p>Design, plan, organize and evaluate trainings and exercises, provide feedback</p> <p>Ability to include balanced cost and risk mitigation measures.</p>
Communities and Stakeholders	<p>Continuous involvement through LCN</p> <p>Introduce local knowledge, culture, social perspectives and related programs.</p> <p>Leverage and identify local resources that could be mobilized</p> <p>Provide information on potential risks, acceptable risks levels and possible/practical mitigation.</p> <p>Plan / Receive effective risk communication</p>
Security Professionals	<p>Assess vulnerabilities and potential countermeasures.</p> <p>Support physical protection recommendations (including organizational and procedures elements)</p> <p>Support development of multifaceted tools and solutions.</p> <p>On-site security personnel training / curricula / exercises</p>

Designers and Planners (Architect, Landscape Architect, Planner, Urban Designer), Engineers (Civil, Geotechnical, Environmental), IT experts	Work for a long-term development strategy. Develop a strategic, multidimensional, and holistic site design. Work closely with security professionals to create flexible alternatives and innovative solutions. Support collaborative teamwork.
---	---

The identification of the VA team and the exercise for the LCN identification can be run in parallel. Moreover, the SCPM Stakeholder mapping methodology can be used with the Step 1 of the SVA, as an add-on to the legal requirements for the formation of the VA team in the specific context.

Other synergy points could be:

- Include LCN representatives (from the Core Team/Partnership Tier) in the VA team to provide community insights and perspectives.
- Use community forums and workshops to identify suitable candidates for VA team participation.

7.2. Step 2. Plan the SVA

Once the team is assembled, the next phase includes the development of a project plan (by the project management) that outlines how the SVA will be conducted.

Table 4: Indicative Planning Actions.

Step 2. Indicative planning actions
SVA process management and reporting, incl budget issues
Project risk management
Identify local policies / regulations and implement respective procedures
Data gathering, storage and dissemination
Conduct local surveys
Iterative process of SVA development and continuous checking for alignment with local / regional / national policies
Communication with stakeholders and LCN to include socio-institutional and cultural dimensions and their constraints and requirements
Identify and introduce in the SVA risk culture and risk tolerance
Public communication
Acquisition (procurement or other) of tools and hardware for SVA
Identify pertinent KPI

include cross-border cooperation and coordination
Role of LCN
Engage the Partnership and Communication Tiers <ul style="list-style-type: none"> • Organise community meetings to collaboratively define risk tolerance levels • Create accessible risk assessment documents that explain risk tolerance in plain language to LCNs

Within the SVA planning phase it is extremely important to **define the accepted levels of risk and also which security functions will be implemented within the public space / event protection system (Step 6)**. This also guide several decisions needed to implement the SVA assessment and risk prioritization activities.

Another important point that needs to be discussed and acknowledged is that not all threats can be prevented, but identify those that we can be mitigated always taking into consideration underlying constraints. Thus, **critical decisions** need to be made on what threats / vulnerabilities / risk levels are acceptable, by the authorities and the public alike, as it is not always possible to prevent everything, or it would require excessive measures (in terms of costs, personnel, procedures, and technological capabilities) and what mitigating measures to put in place. When physical protection systems are discussed / assessed the team should define **key performance metrics** and other key elements of the system (and also could include their accepted target values).

7.3. Step 3. Define the Threat vector

A vital part of the SVA is to establish a detailed understanding about the threat vectors, those adversaries that could potentially defeat public space security provisions. This process should also include the adversaries' capabilities and attributes, as there is a dynamic evolution of adversary tactics including recent technological advances (e.g. unmanned systems), Within the proposed SVA the following options could be used:

7.3.1. Identification of adversary registry

Establish an initial registry of adversaries and malevolent activities from existing open source data bases, interfacing with national agencies and LEAs, etc.

Table 5: Potential list of adversaries.

Malevolent act	Description
----------------	-------------

Unauthorized entry	Access to protected / closed areas by non-authorized persons
Civil Disturbance	Disruption of community function that requires intervention
Vandalism	Acts of destruction of public space objects
Theft / Robbery	Unauthorised removal of valuables
Fire arms attack	Attack using small pistols or automatic rifles
Sharp object attack	Sharp and blunt objects (e.g., knives)
Vehicle Attack	Vehicle as a weapon e.g. ramming large crowds
IED	Any type of explosives in objects or goods
PBIED	Explosives concealed on a person (e.g. suicide)
RC/UAS – IED	Remote controlled or UAS delivered explosive device
VBIED	Vehicle born explosive devices
Chemical attack	Toxic or harmful chemical in goods or carried items
Biological attack	Deliberately released biological pathogen
Radiological attack	Deliberately released radioactive material as is (RED - exposure device) or combined with dispersal material (RDD – dispersal device)

Other types of attacks can be considered

7.3.2. Characterization and ranking of adversaries

Under the proposed SVA the adversaries could be characterised through (Figure 9):

- Its **Intention** to harm, which can be further analysed into two components: (i) the desire to realize the threat (e.g. including likely attitude for themselves being exposed to the said risks, e.g. chemical agents) and (ii) the motivation to pursue an appropriate course of action towards realizing the threat
- Existing **capabilities** to carry out the threat effectively: (i) resources (human, material, technical, logistics, financial etc. needed for execution of a threat plan) and (ii) collected knowledge (facility, attacking, planning, logistics) required to mobilize resources and to inform the plan with vulnerability data to carry out the threat effectively

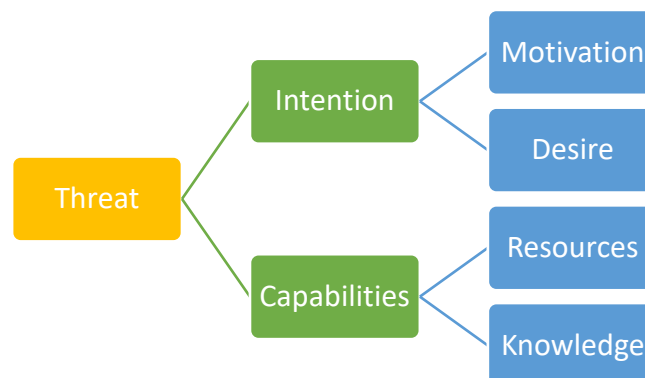


Figure 9: Threat characterization.

Each of the identified adversaries can be further categorised in terms of its Intent and Capabilities using different categorical scale values as for example in Table 6.

Table 6: Threat categorization.

Scale	Motivation	Desire	Resources (material, funding)	Knowledge (Training)
Very Low	No expectation to succeed	Little or no desire	Few , if any	None
Low	Limited capacity to succeed	Use peaceful means	Limited	limited
Medium	Reasonable expectation to succeed	Flexibility for methods used	Moderate	Moderate
High	High expectation to succeed	Limited room to compromise decisions, tend for extreme actions	Significant	Skills and training
Very High	Sure to succeed	No room for compromise, potential suicide	Fully	Military / SOF training

7.3.3. Implementation of the design basis threat (DBT)

In parallel to the identified and categorised assessment of the potential adversaries this set of attributes and characteristics can be used to form the basis for designing the physical protection systems, known as the **Design Basis Threat** (DBT). DBT establishes a profile of the type, composition, and capabilities of adversaries. It is an estimate of the threat across a range of undesirable events and is usually based on the best available information, reports, assessments, and crime statistics at the time of the SVA.

Table 7: DBT contents.

Type	
Motivation	Political, financial, ideological, personal
Adversary Number(s)	Total number of adversaries, focusing on those directly participating to the attack, and noting people indirectly participating / aiding (also include insiders)
Insider	Indicate type (could be multiple types) : active / passive / witting
Knowledge	targets, site plans and procedures, security measures, safety measures

Willing to Kill/Die	Yes / no
Weapons	types (knives, Fire arms, etc), numbers, availability
Explosives	Type (incl VIED, PBIED), quantity, availability, triggering sophistication, acquired or improvised
Tools/equip	mechanical, thermal, manual, power, electronic, electromagnetic, communications, etc
Transportation	Type(public, private, land, sea, air) number, availability
Technical Skills	engineering, use of explosives, chemicals, paramilitary experience, communications skills
Cyber Skills	computer and automated control systems in direct support of physical attacks, intelligence gathering, cyber-attacks, money gathering
Deception/Diversion	use of stealth, deception, or force
Support/Planning	Support organization, logistical support

7.3.4. Emerging Threat landscape – Unmanned Systems

This document refers also the findings in ENLETS ETP Program Countering Unmanned Aircraft Systems Final Report 2022 (ENLETS2022). The ENLETS C-UAS TIG Group is a continuation of the previous ENLETS Drone Technology Interest Group 2016 - 2020. The experience gathered in the Drone TIG appeared crucial to understand the operational concepts and potential threats caused by UAS's. The ENLETS C-UAS TIG is supported by Advisory Board made up of representatives of DG HOME of the European Commission (Unit D.2 Counter-Terrorism).

Along with different benefits the drones also produce different effects. After several years of active consideration to drones from security and safety perspective of LEA, we can see that the unmanned systems are causing opportunities but at same time **new kind of threats in society** for public and private properties.

At the moment from Counter-UAS perspective, we have different puzzle pieces of response from different stages, but a whole chain that starts with the observation of the target and ends with the choice of the target being able to be taken down safely is still under the research. Likewise, our strong assumption is that at present the various detection systems need a comparative observation system alongside each other to support each other in order to obtain the best possible situation in the environment. This will ensure a better perception of the sites around. At same time the law, fundamental right to fly and privacy are causing limitations to use the technology and observe the environment efficient way.



Figure 10: Helsinki, (picture by Finnish police).

Regulations have developed stricter for UAS's pilots in EU area in last years (Seasar2017). On nowadays UAS operators are obligated to register. This goes for both professionals and leisure time pilots. There were 20 166 registered UAS pilots in Finland (including professionals and leisure time users) on January 1st, 2023. Law enforcement authorities estimates that true number of UAS pilots is presumably much higher in Finland as every other EU state comparing the official registration numbers.

The recent study by JRC (2023) identifies the following list of potential scenarios where UAS could be employed, although potentially different imaginative ways could be considered in such assessments:

- **Transfer of hazardous loads**, including CBRN, explosives and used directly and/or indirectly as attack carriers.
- **Smuggling/delivery**, for delivering equipment / illicit material at specific locations
- **Intelligence gathering**, surveillance and reconnaissance, mainly through the use of cameras or other sensors
- **Cyberattacks**, by targeting local wireless networks, disrupting communications, delivering malware, hijacking and/or manipulating sensitive data
- **Jamming**, appropriate electronic equipment onboard may be used as a local jammer to interfere with perimeter security systems, GPS / mobile phone signals.
- **Disruption and interference**, even the presence of a UAS may be enough to interfere with the normal operations (e.g. civil aviation).

Interaction with LCN

- Establish a community-driven threat monitoring system to collect local threat information.
- Involve LCNs in threat analysis through regular threat perception surveys and interactive online platforms.

7.4. Step 4. Characterization of the public space

This process involves identifying and understanding the overall public space role in urban life including societal, urban planning, and its physical condition. All information and data collected will be used to fully understand **what must be protected** (targets – step 5), **from whom** (threats – step 3), and to **what performance** (step 6) which is directly linked to the **determined risk tolerance level** (step 2).

Interventions on public spaces embedding safety principles and goals into the design choices should be intended as complementary to other more traditional approaches to urban security, based respectively on the maintenance of public order through the law and the presence reinforcement of the forces of order; and on interventions at social level, aiming at the reduction of conditions of disadvantage and deprivation, considered as a factor increasing the risk of criminal acts.³⁰

Table 8: Security by Design principles.

SAFE-CITIES security – urban planning interface
Avoid an oversensitivity to risk (and, consequently, ensure a proportionality between measures and potential risks) ³¹ , ensuring a balance between safety/protection and open nature of public areas/openness ³² ;
Integrate security/safety into the planning and design processes, based on shared informed decisions following more collaborative and inclusive processes among as wider as possible stakeholder groups; ³³
Combine the creation of barriers or boundaries with a physical design of the space and integrate additional protection according to existing layout/asset able to prevent risks and threats ³⁴ and in order to respect and complain with its function, social and symbolic value;
Consider security measures from the early stage of design process (avoiding exclusively barrier solutions) in order to complain with an integrated vision of 'beautiful, sustainable and inclusive' public spaces, in line with the New European Bauhaus principles; ³⁵
Consider the adoption of standardized urban furniture (e.g., benches, bollards, rails and fences, and natural barriers, in some cases specifically certified) as well as ad-hoc protective measures (e.g., public art), promoting multifunctionality and ensuring a balance between elements; ³⁶
Consider the presence of physical measures in the streetscape for specific attacks, combining general planning principles, attention to access points and boundaries, identify sensitive points, identify targeted routes and access points

30 Bolici, R., Gambaro, M. (2020), "La sicurezza urbana per la qualità dello spazio pubblico", *TECHNE* 19, pp. 105-106.

31 Home office of Great Britain (2014). Protecting crowded places: design and technical issues.

32 Nadel, B. A. (2004), *Building security: Handbook for architectural planning and design*. McGraw Hill Professional, New York.

33 European Commission (2022), *Security by Design: Protection of public spaces from terrorist attacks*, 2022, p.26.

34 Perspective.brussels, Department Territorial Strategy (2019, October), *Guide to the integration of security systems in public spaces, Brussels-Capital Region*, p.27.

35 European Commission (2022), *Security by Design: Protection of public spaces from terrorist attacks*, 2022, p.26.

36 Perspective.brussels, Department Territorial Strategy (2019, October), *Guide to the integration of security systems in public spaces, Brussels-Capital Region*, pp. 19-34.

Concentrating **vehicle flows** with specific systems to be integrated into the public space providing/defining obstacles and surveillance measures 37

Design **climate and environmental mitigations** solution (e.g., plants, water retention devices, etc.) in a multifunctional way to serve as a protective measure. 38

7.4.1. Categories of Public Spaces of relevance to SAFE-CITIES

Public spaces are closely linked to the people's leisure and quality of living and may carry economic, commercial, cultural, historic, religious, archaeological value or constitute a point of geographical reference with high concentration of people. These may include closed or open areas such as transport hubs, open squares, parks, shopping areas, nightlife areas, cultural venues, business venues, places of worship, or institutional venues/buildings (see table 5). Technically, some public spaces are semi-public spaces and are privately-owned or privately-operated spaces (e.g., train/metro stations, shopping malls). The categorization below is based upon the ???

Having that in mind, and in agreement with the (COM 2017) EU's "Action Plan to Support the Protection of Public Spaces" approach. all the provided examples included in Table may be considered as public spaces due to their importance and the impact on the citizen's.

Table 9: Public Space Categorization (list in alphabetic order).

Public Space Type	Examples
Business	Hotels, large office spaces, conferences
Cultural	Concert hall, museum, monuments, sport events, stadiums, amusement parks, tourist sites, etc
Institutional spaces	Public buildings, healthcare buildings, education buildings,
Nightlife areas	High density of bars, pubs and/or nightclubs, restaurants, coffee shops, small concert halls
Religion / Worship	Churches, mosques, etc
Shopping areas	Malls, main shopping streets in city centres
Squares	Squares were many events take place, next to important buildings, have regular big markets, festivals, etcetera.
Transport hubs	Train station, bus hub, underground metro stations, airports, etc.

The public space may refer to any public space which is generally of open access to the public. Also, semi-open or controlled access (closed) spaces, such as roads, parks, squares, libraries, metro stations, municipal buildings and others, with low or high concentration of people, whether this occurs on daily basis or due to a specific event, can be considered.

37 Ibidem.

38 European Commission (2022), *Security by Design: Protection of public spaces from terrorist attacks*, 2022, p. 34.

7.4.2. “Open”, “semi-open” or “closed” spaces

Public spaces can be categorized as **“open”**, **“semi-open”** or **“closed”**, linked to the control of accessibility, depending on the case (e.g., closed privately owned vs open public owned areas). Unlike privately owned buildings/areas with restricted access, the open and uncontrolled access may result to looser security measures in an effort to avoid interference with a site functionality and aesthetics, to avoid legislation and ethical issues, or to avoid causing a sense of fear and insecurity to the public.

However, the lack of security measures may render a public site vulnerable to manmade threats such as potential terrorist attacks or regular criminal activity. The identification of security gaps through systemic analysis may provide the ability to make risk-informed decisions to adopt smart security measures in harmony with the security, functional requirements, and the type of a specific public space of interest.

Interaction with LCN

- Develop community-led surveys and focus groups to gather insights into the societal importance and functions of public spaces.
- Engage LCNs in the collection and analysis of this data.

7.5. Step 5. Identify the Targets and quantify their attractiveness.

Target analysis involves the identification and characterization of the importance of public spaces that must be protected to ensure a high level of security system effectiveness against defined threats. This attribute – target attractiveness - can be quantified using commonly obtained parameters and can be an effective means of ranking different areas within a city against a common system. *Table 10* describes the different attractiveness factors that were proposed within the SAFE-CITIES project and a potential classification scheme based on a 5-level categorical scale

Table 10: Public space attractiveness factors.

Title	Description	Very Low	Low	Medium	High	Very High
Media	Media exposure of public space / event	Occasionally in regional / local news	Frequently in regional / local news	Occasionally in national news (less than 1 time per year)	Frequently in national news	Global news coverage
Knowledge	If someone can find information about the public space	Sparse information is available	Detailed information only on architectural / urban plans	Detailed information only on security provisions	Some information on both urban / architectural	Detailed information on both urban / architectural

	event in open information space				plans and security provisions	plans and security provisions
Criticality	How critical is the public space / event for life in the city	The public space will continue to be used after a security incident	Changes need to be made in daily life to accommodate response / recovery to a security incident	Public life could be disrupted for some hours (up to 1 day)	Important, some activities and services could be stopped (indicatively <3) and for more than 1 day	Very important, other activities and services could be stopped (indicatively >3) for more than 1 day
Symbolism / Iconic Value	The public space event has a unique Cultural Value	Individual or some communities scale value (for some communities - citizens)	Local scale value (for all communities - citizens), local religious site	Site has a regional scale symbolism, religious site	National heritage, religious sites	Global Importance (UNESCO site)
Existing protection	Assessment of the level of protection	No or minimal protection only by local police	some basic surveillance system linked to local police	Only one of (National Police - Local Police - Private sector) and no type of surveillance system	National Police and/or Private sector and some type of surveillance system	National Police and Private sector and automated surveillance system
Accessibility/ Escape	How easily an adversary (group) can access and escape the site	Public space has single access and one escape route that can be blocked	Public space has single access and one escape route that can't be blocked	Public space has few access roads and potential escape routes can be blocked with some difficulty	Public space has few access roads and potential escape routes can't be blocked	Public space has many access roads and potential escape routes can't be blocked

Interaction with LCN

- Develop interactive tools that allow community members to rate and comment on target attractiveness factors – for instance use of Mapotic platform(www.mapotic.com).

7.6. Step 6. Describe the public space security system

The main goal of the security assessment is to identify the current security measures and practices in place, and the VA will identify the weaknesses (vulnerabilities) of the public space against specific threats. The effectiveness of the existing security

measures is indirectly introduced in the risk assessment process as they may affect the likelihood of threats and their potential impact.

A detailed security system characterization includes identifying public space security elements that provide **detection, assessment, delay, and response capabilities**. A thorough on-site survey allows security specialists to identify all protection elements and collect performance data for each component and the system as a whole. Presently physical protection and security systems of public spaces have four core functionalities that include:

- **Deterrence:** means that a perpetrator refrains from carrying out the attack on the intended site. The design of the security measures means that the perpetrator deems that the risk of failure is too great, which may also mean that the perpetrator does not have the whole picture of which security measures have been implemented.
- **Detection:** means security measures aim to verify that an attack is under way and to provide decision input for early and timely response.
- **Mitigation:** means reducing adversary's possibilities of carrying out a successful attack and mitigate the consequences of the attack.
- **Response:** means measures intended to stop and discontinue an attack, mainly by security personnel or the police.

Additionally, the public space protection system needs to consider the different functions and security operations, the security processes and the different stakeholders. Contextualizing the role of the stakeholders, both in the design of the PPS and the implementation of the SVA, Figure 11, can result in the identification of potential security breaches by man-made threats, and the identification and analysis of vulnerabilities of selected public spaces, in relation to the threats identified. Table 11 describes the main functionality that has been introduced in the ISF-PROTECT project.

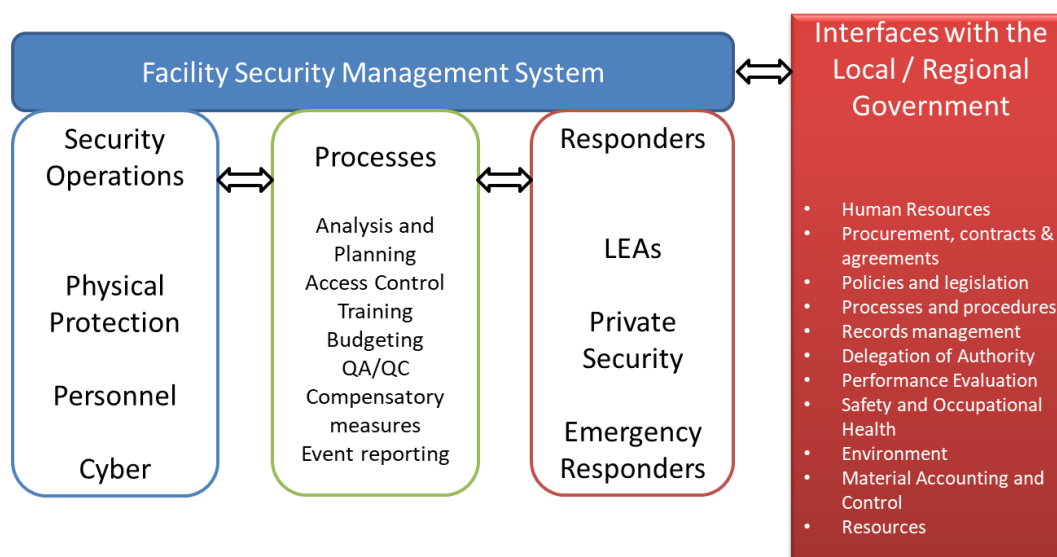


Figure 11: Overview of Public Space physical security regime.

Table 11: Security Function according to PROTECT – project.

Function	Detailed
ALERT	Place Visual signs alerting public from parking or driving or approaching the specific zones, large signs alerting the public of approaching security controls
SURVAIL	Placement of identifiable and covert Police vehicles in the areas which have the largest vulnerability
DETECT	Strengthen access control and consider temporary explosive detection checkpoints to randomly search persons. Deployment of CCTV cameras in parking / perimeter and regular monitoring
PROTECT	Placement of movable barriers to restrict access and also consider the placement of concrete barriers to mitigate against vehicle threats
OVERCOME	If certain measures not available, use temporary solutions (ex. temporary deployment of CCTV (cameras) in the critical areas - even "fake" CCTV can result in deterrence)
RESPOND	Deployment of more police teams in the stadium perimeter, and could also consider special units and other rapid response force. Deploy mobile patrols. Place ER vehicles and teams

7.6.1. SAFE-CITIES public space security integrated policies functions

Within the SAFE-CITIES we propose a more elaborative approach where the following layered security provisions could be selected. A set of foundational security policies are proposed each linked to security functionality / measures which can be developed to support the protection of public space, supported by horizontal implementation measures.

Layer 1: Public Space security policies (PSS). PSS are the foundational security principles that establish how each public space must be protected and determine public space protection measures. Within the SAFE-CITIES framework they should represent a core set of principles guiding the protection of public spaces.

Layer 2: Public Space Protection measures (PSPM). PSPM are collectively focused on the delivery of effective public space security that is linked to the security plan of the public space / city. PSPM linked to PSS 1-5 are concerned with enabling the delivery of effective security, whilst those for PSS 6-10 are concerned with the delivery of security operations

Table 12: Public Space security policies and functions.

ID	Policy	Description
PSS1	Leadership and Management for Security	Establish implement and maintain organisational security capability supported by strong leadership, robust governance, and accountability of security arrangements
	PSPM1.1	Governance and Leadership
	PSPM1.2	Capable organisation for public space security
	PSPM1.3	Rigid decision making
	PSPM1.4	Organisational learning
	PSPM1.5	Assurance processes
PSS2	Organisational Culture	Establish organisational culture that promotes the importance of security
	PSPM2.1	Maintenance of a Robust Security Culture
PSS3	Management of Human Capacities	Ensure the human capacities public space security is understood and appropriately designed, including regular training
	PSPM3.1	Identification and Analysis of Tasks and Roles
	PSPM3.2	Sufficiency and Competence of Persons Delivering Security
	PSPM3.3	Suitable and Sufficient Workspaces, Equipment and User Interfaces
	PSPM3.4	Suitable and Sufficient Procedures and Administrative Controls
PSS4	Enablers Management	Establish the necessary environment for enabling conditions to support public space security: procurement of products or services, supply chain management
	PSPM4.1	Procurement and Intelligent Customer Capability
	PSPM4.2	Supplier capability and availability
	PSPM4.3	Oversight of Suppliers of Items or Services
	PSPM4.4	Commissioning in service
PSS5	Reliability, Resilience and Sustainability	Establish a security regime that is reliable, resilient and sustained
	PSPM5.1	Business continuity and capacity to overcome failures and improvise
	PSPM5.2	Systematic examination, inspection, maintenance and testing
	PSPM5.3	Sustainability over time
PSS6	Physical Protection Systems	Operate PPS that integrates technical and procedural measures and are graded according to the potential impacts of a successful attack
	PSPM6.1	Physical protection system design
	PSPM6.2	CPTED principles
	PSPM6.3	Vulnerability assessments
	PSPM6.4	Security function: ALERT

	PSPM6.5	Security function: SURVAIL
	PSPM6.6	Security function: DETECT
	PSPM6.7	Security function: PROTECT
	PSPM6.8	Security function: OVERCOME
	PSPM6.9	Security function: RESPOND
PPS7	Cyber Security & Information Assurance	Establish effective cyber security and information assurance arrangements that integrate technical and procedural controls
	PSPM7.1	Effective Cyber and Information Risk Management
	PSPM7.2	Information security
	PSPM7.3	Physical Protection of Information
	PSPM7.4	Preparation for and Response to Cyber Security Incidents
PSS8	Workforce Trustworthiness	Establish workforce trustworthiness to reduce the risks posed by insider activity
	PSPM8.1	Cooperation of competent authorities
	PSPM8.2	Pre-employment Screening
	PSPM8.3	Ongoing personnel security
PSS9	Policing and Response Teams	Effective policing arrangements integrating the operations of relevant leas and security guards
	PSPM9.1	LEA role
	PSPM9.2	Security guard
	PSPM9.3	Emergency responders
	PSPM9.4	Local citizen networks
PSS10	Emergency Response	Establish effective Emergency Response arrangements which are integrated with the wider protection and safety arrangements
	PSPM10.1	Emergency response planning
	PSPM10.2	Testing and exercising
	PSPM10.3	Clarity of Command, Control and Communications during an incident

7.6.2. PPS design considerations

Best practices for public space security design includes the selection of elements that support security functions in multiple ways, by providing the following:

- **Physical deterrence**, as for example hardened perimeter elements enforcing the standoff zone, the distance between potential explosions and the public space under consideration.
- Establish **access restrictions**. Ensure that unauthorised personnel are not in areas not accessible to the public and consider accessing control and security checks when appropriate
- **Psychological deterrence**, having the ability to design very obvious and almost forbidding security measures and for other public spaces, more subtle approaches that do not call attention to the site as a potential target.
- **Support for observation, surveillance, and inspection**. Allow sight lines and vistas that provide natural opportunities for observation of those approaching the public space, or to block views of sensitive areas. Camera surveillance and

monitoring by security personnel can deter a perpetrator or expose preparations.

- **Protective measures** against explosives, which is usually is to increase the distance between what is to be protected and the presumed attack site. Another measure may be to reduce the effect of fragments from glass in (surrounding) buildings, or enforce sufficient resistance to explosions.

7.6.3. Counter UAS

Many member states are facing crucial challenges matching countermeasures to their legislation. For instance, LEA's must have legitimacy to handle the data of the UAS (GDPR) and laws changing process regarding UAS's takes quite some time. As technology keeps evolving, it is mandatory to think ahead and look at potential physical security measures Table 13.

Table 13: Counter UAS list of measures.

Category	Measure
Detection, tracking and identification	Radars
	Radiofrequency scanners
	Acoustic sensors
	Daylight /thermal cameras
Interception / neutralisation technologies	RF Jammers
	Spoofing
	Lasers, HPM, EMP
	Expendable UAS, Projectiles
	Deployable nets
	Birds of prey
Physical Hardening Measures	Geofencing
	Blast resistant windows/facades
	Anti-shatter films
	Laminated glass
	Catching systems
Netting/fences	Top floor slab
	External building skins
	Attenuation solutions
Concealment and repositioning	
Awareness raising, geofencing and identification potential	

7.6.4. Community Policing

Community policing is a strategy of policing that focuses on building ties and working closely with members of the community through interactions with local agencies and members of the public, creating partnerships and strategies for reducing crime and disorder. The concept is traditionally used by local LEAs that have a direct impact on everyday security of a community and affect citizen quality of life. This approach is commonly used as a form of gathering intelligence. The interaction between the police and the public can provide an important source of information and therefore guide the actions of the LEAs. Through the effective implementation of this concept citizens can become key players and reliable partners to “co-produced” security.

Interaction with LCN

- Use community workshops and virtual tours to involve LCNs in the description of the security system.
- Create user-friendly visual aids and infographics to help LCNs understand the security measures in place.

7.7. Step 7. Conduct risk assessment

A main outcome of the SVA is the risk assessment which involves the quantification of the threats for specific public space, that needs to consider a) a determination of the likelihood of the assessed threat to conduct the attack and b) the multi-dimensional determination of the impacts of the public space, society and security stakeholders should the attack is successful. Usually, all the different examined risks are quantified through semi-empirical (e.g. through a risk matrix) and probabilistic models, and are ranked based on determined scores/values.

When concerning the **likelihood dimension** of the attack three options are proposed

Likelihood quantification option 1. Obtain historical and risk data from national agencies and subject matter experts and link them to the likelihood categories in Table 15

Likelihood quantification option 2. Use the scales of the threat quantification Table 6, and those criteria to map them to the likelihood categories in Table 15, based on some weighting average process.

Table 14: Potential Impact factors.

Title	Description	Very Low	Low	Medium	High	Very High
Political impacts	New legislations, changes of organizational processes, political views (security perceptions)	Low political interest	Identification of need to implement changes in security culture	Steps to implement security culture (e.g. training) in organization	Changes in security processes within organization	New legislation resulting from incident
Societal impacts	Disruption to societal functioning	Few people whose daily routine is disrupted	Medium number of people whose daily routine is disrupted (10<people<500) and impact lasting less than a week	Medium number of people whose daily routine is disrupted (10<people<500)) and impact lasting more than a week	Large number of people whose daily routine is disrupted (>500) and impact lasting less than a week	Large number of people whose daily routine is disrupted (>500) and impact lasting over a week
Reputation	Impact on the reputation of the city or incident location	Sporadic comments on security provisions	Negative comments in media and social media	People will likely stop using the public space /not go to event	People will cancel participation in events	People will stop using the public space
Environmental damages	Impacts to the environment and ecosystems	Area fully restored within a day	Area fully restored within a week	Area fully restored between 1 week and 1 month	Area fully restored between 1 month and 1 Year	Long lasting environmental impacts >1 year to fully recover
Critical services	Number of critical services (utilities, societal, government) stop functioning	All services restored within 1 day	<3 critical services less than 1 week	<3 critical services more than 1 week	> 3 critical services less than 1 week	> 3 critical services more than 1 week
Economic Loses	Total economic losses quantified in Euros (or other currency)	< 10K euros	between 10 and 100K euros	between 100 and 500K euros	between 500k and 5M euros	>5 million euros
Destroyed buildings	Number of buildings exposed to the attack (and also those potentially damaged)	<10 buildings exposed	between 10 and 100 exposed - minor damaged	> 100 exposed and minor to damages that can be repaired with occupants inside	>10 damages with temporary relocation needed	>5 beyond repair
Crowd density	Number of people potentially exposed in the attack per square meter unit -	<0.01 per sq. meter	0.01-0.1 per sq. meter	0.1-0.5 per sq. meter	0.5-2 per sq. meter	>2 per sq. meter

	not necessarily casualties or otherwise injured					
--	---	--	--	--	--	--

Once the levels of the severity and likelihood of a successful threat scenario have been assessed, through a categorical scale, **the risk level** of each scenario can be determined with the help of a risk matrix which quantifies the level of risk and provides a link to the acceptability of each security risk and a relative ranking between different risk and public spaces in region. Examples (Table 15) include a risk matrix, with 5 levels of risk

Table 15: Example 5x5 Risk matrix.

	IMPACTS					
		VERY LOW	LOW	MED	HIGH	VERY HIGH
LIKELIHOOD	VERY HIGH					
	HIGH					
	MED					
	LOW					
	VERYLOW					
RISK LEGEND		VERY LOW	LOW	MED	HIGH	VERY HIGH

Within this table, and based on the perceived risk levels (Step 2), non-acceptable level of risks can be defined which is an indication for further improvement in countermeasures (risks assigned a red colour); an acceptable level of risk (assigned a green colour) where it is considered that sufficient countermeasures have been implemented for the threat scenario.

Interaction with LCN

- Develop an online risk assessment platform where LCNs can provide input on risk likelihood and impacts.
- Provide training sessions and user manuals to support LCNs in using the platform effectively.

7.8. Step 8. Scenario Building: Determine the most vulnerable path and develop worse-case scenarios

The site data collected, and assumptions reached in order to implement Step 4 and Step 6 are used to construct models for credible “attack pathways” from outside the public space to the selected targets areas. Different types of assessments that could include:

- a) expert analysis, e.g. narratives and short stories, based on site surveys,
- b) table top exercises and
- c) advanced computer models such as the SVA scenario builder.

Using site collected data it is possible to quantify each path, and the results to be used for the determination of the most vulnerable and accessible paths and potential attackers' detection points.

Although different risk scenarios could be used for this assessment, the majority of the analysis **are based on “worst-case scenarios”**. Within this assessment it is possible to identify detection probabilities (by both human and surveillance systems), interruption points and path delays. All potential and credible attack options are studied to ensure that worse-case attacks and other serious options that need to be protected against are identified.

7.8.1. Path analysis

All potential and credible attack options are studied to ensure that worse-case attacks and other serious options that need to be protected against are identified. For the analysis, attack scenarios are described in a highly detailed step-by-step process, including phases before – during – after the attack including the implementation of the security functions of Table 12. In order to conduct this assessment the following phases should be performed:

Phase 1: select the attack vector, based on SVA step 3

Phase 2: describe the public space, SVA step 4, and the most potent target from the target attractiveness assessment, SVA step 5

Phase 3: introduce the security functions, SVA step 6.

Phase 4: perform path analysis and evaluation of the performance of the security system. Three main actions are concerned:

Phase 4.1: evaluated by simplifying the using an adversary sequence diagram (ASD) for the identified potential target

Phase 4.2: Conduct path analysis which determines critical detection points, identifies areas where the attack may be interrupted and/or delayed and the adversaries detained / neutralised.

This process provides a functional representation of the security provisions of the public space, describing the elements and their functional properties (Table 12) but the analysis should go beyond just representing the cyber/ physical systems and include communication and decision-making processes and respective times.

The path analysis uses estimated performance measures, according to the physical protection system design – SVA step 6 - to assess weaknesses along all credible adversary paths into the public space, measured by some pertinent metrics like probabilities of implementing (or failures of) the security functions.

A scenario analysis is conducted to determine the security system vulnerabilities, considering not only the static dimension but most importantly the dynamics of the adversary. According to the SAFE-CITIES SVA principles, the dynamic – scenario based VA is equally important as it may reveal weaknesses to a perfectly designed security system, according to functional requirements. The most notable example is that responders may arrive late in the scene, although the detection and identification systems and process worked according to design.

The scenario analysis process should also consider different operating conditions and modalities of the public space and the security system. A recommended way to overcome this is the use of “worse-case” scenarios.

Interaction with LCN

- Organise scenario-building workshops involving LCNs to identify potential vulnerable paths.
- Create user-friendly software tools that allow LCNs to map out and visualise scenarios.

7.9. Step 9. Responding to the threat

This step consists of the activities needed in order to respond to the security threat, that for the purposes of this assessment have been split into three sections presented below:

7.9.1. Attack Interruption and Neutralization

This analysis is a continuation of the scenario building phase – SVA step 8 – and it should provide information about how effective the response force will be at detaining / neutralizing the threat using the identified worst-case scenarios. The assessment should evaluate the physical protection measures and of the physical protection system,

including the timely response of the security personnel and LEA response forces. This assessment can be conducted using

- Simple methods based on data about: adversary numbers - capabilities, and equipment and response / security personnel numbers - capabilities, and equipment
- More complex methods that require data for: Initial locations, path analysis, final locations of security/response force and the adversaries, and also terrain, building schematics, PPS characteristics
- Probabilistic models for assessing the neutralization probabilities for different combinations of “equally armed” security personnel and adversaries
- Simulations and TTX could be used to predict the probability of neutralizing violent adversaries after interrupting them.

Some of the factors that can be used in the neutralization assessment include:

- Numbers of responders
- Weapon superiority, where more advanced weapons increase the rate of attrition that one side can cause on another side
- Regular and Special Forces Time
- Effects of force multipliers, such as the number of casualties caused at an access control point from adversary use of a vehicle bomb
- Tactical decision-making process
- Command and control operationality
- Training and tactics to respond to the adversary.

7.9.2. Emergency Response Actions

Within SAFE-CITIES, a key recommendation from the Gdansk workshop, was to integrate emergency response to the identified scenario. It was decided to include the phases following the termination of the adversary activities (as described in section above). Of course the proposed analysis here is indicative and to a large extent generalising on partners input and provided experiences.

The emergency response to public spaces security incidents, especially those of “medium impact” - Table 14, require arrangements by emergency services and include the involvement, either directly or indirectly, of large numbers of people, performing additional functions such as:

- the mobilization of resources of emergency services and support services

- the traffic arrangements
- the rescue and transportation of a large number of casualties
- the handling of a large number of enquiries likely to be generated both from the public and the news media (usually made to the police).

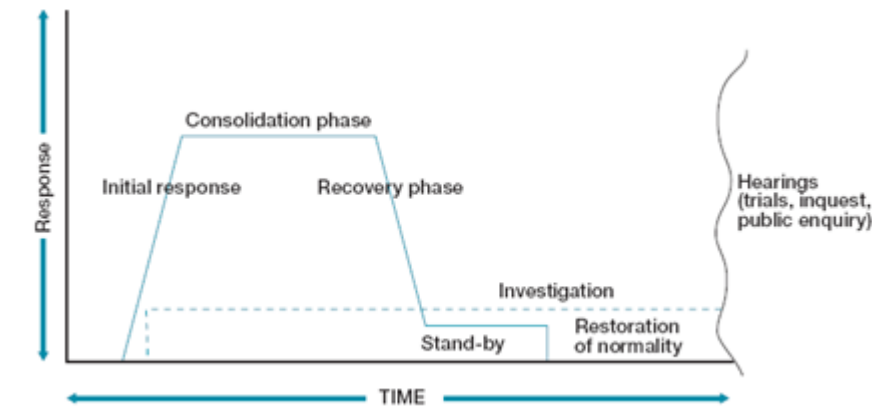


Figure 12: Time stages of public space security scenarios.

Usually the emergency response occurs in the consolidation and recovery phase, Figure 12, for the safety of the emergency personnel and such assessments should not only include emergency responders but also the cyber / physical emergency response infrastructures and consider intrinsic geospatial attributes:

1. Emergency response infrastructures are interconnected, thus securing one infrastructure will diminish the impact of other infrastructures
2. Emergency response infrastructures, under most conditions, are heavily reliant upon each other.
3. Emergency response infrastructure is, by and large, portable and is highly dependent upon local infrastructure during a time of crisis.

In addition to the deployment of the emergency responders, scene management provisions should be considered. Usually these are organized through cordons, established around the public space for the following reasons (a) to guard the scene (b) to protect the public (c) to control sightseers (d) to prevent unauthorized interference with the investigation (d) to facilitate the operations of the emergency services and other agencies, Figure 13.

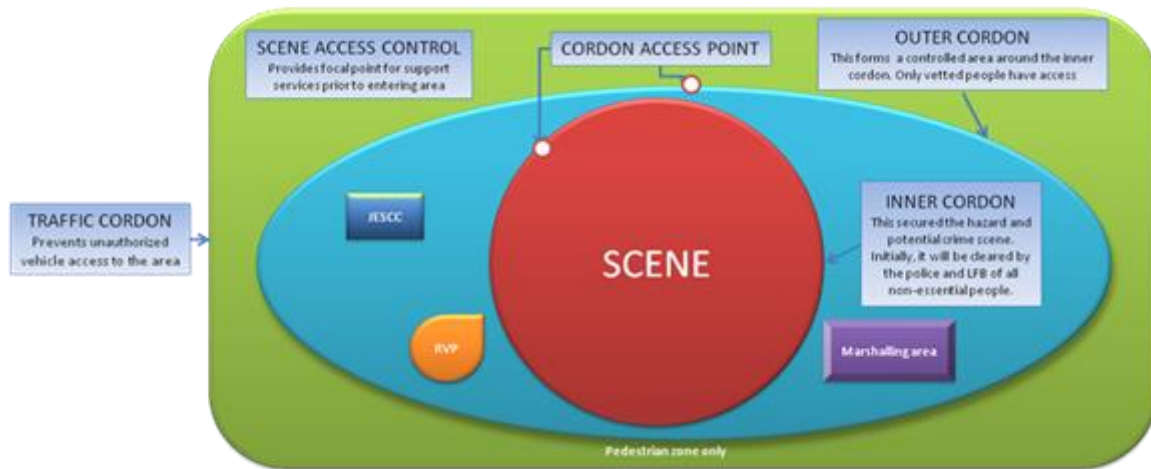


Figure 13: Scene management.

Usually, a procedure with three cordons will be established. This will be done commonly by the police in consultation with other agencies, Figure 13, in summary, the following cordons will be formed.

- inner cordon – provides immediate security of the hazard area and potential crime scene;
- outer cordon – seals off an extensive area around the inner cordon; and
- traffic cordon – set up at or beyond the outer cordon to prevent unauthorized vehicle access to the area surrounding the scene.

As exemplary, we introduce prominent roles and functions of the main emergency response teams that could be intervening in public space related threats.

Police

The primary areas of police responsibility are subject to national legislations and local operating procedures, and indicatively could include:

- maintenance of safe conditions together with the other emergency services
- acting in support at the scene of the incident
- secure, protect and preserve the scene and to control sightseers and traffic through the use of cordons
- investigation of the incident and obtaining and securing of evidence in conjunction with other investigative bodies where applicable
- collection and distribution of casualty information
- short-term measures to restore normality after all necessary actions have been taken

Fire Brigade

The areas of responsibility of the fire brigade are subject to national legislations and

local operating procedures, and indicatively could include:

- life-saving through search and rescue;
- firefighting and fire prevention;
- rendering humanitarian services;
- detection, identification, monitoring and management of hazardous materials and protecting the environment;
- salvage and damage control;
- reinstatement of a state of normality at the earliest opportunity

Ambulance Service

The areas of responsibility for the Ambulance service are subject to national legislations and local operating procedures, and indicatively could include:

- save life together with the other emergency services;
- provide treatment, stabilisation and care of those injured at the scene;
- provide appropriate transport, medical staff, equipment and resources;
- establish an effective triage system to determine the priority
- evacuation needs of those injured and to establish a safe location for casualty clearing,
- provide communication facilities for health services resources at the scene, with direct radio links to hospitals, control facilities and any other agency as required;
- nominate and alert the receiving hospitals from the official list of hospitals to receive those injured and to inform the other agencies;
- provide transport to the incident scene for the Medical Officers, mobile medical/surgical teams and their equipment;
- arrange the most appropriate means of transporting those injured to the receiving and specialist hospitals;

Local authority

The areas of responsibility for Local Authorities are subject to national legislations and local operating procedures, and indicatively could include:

- providing support and equipment for the emergency services;
- providing support and care for the local and wider community;
- using resources to mitigate the effects of an emergency; and
- During a major incident local authorities will act to maintain their normal day-to-day services to the local community.
- All local authorities employ emergency planning officers who are able to plan for and coordinate the local authority response to such events.

LCN

There are numerous LCN which can contribute towards the successful response to an incident. Their support at an event can often alleviate some pressure on the statutory bodies by providing support services. This is especially so during the consolidation and recovery phases when fire, police and ambulance personnel are fully deployed elsewhere.

7.9.3. Radiological Event Response

For the provision of emergency response process to security scenarios covering radioactive substances, each nationally mandated agency has established localized provisions and response capacities. For the purposes of assessments related to SAFE-CITIES, we adopted the generic procedures proposed by the International Atomic Energy Agency (IAEA) in the document: Nuclear security systems and measures for major public events : implementing guide (IAEA 2012)

The main challenge in assessing, preparing and responding to Radiological events have to do with their nature that calls for specialized knowledge during prevention, presence of specialized equipment for detection and alerting, a different concept of operations for response.

Nuclear and other radioactive material can generally be **detected** by instruments without intrusive search by using various kinds of specialized radiation detection instruments available commercially. The deployment of detection instruments at prioritized strategic locations should increase the probability of detecting the presence of nuclear and other radioactive material. The effectiveness and efficiency of these systems will depend on the type and the numbers of radiation detection instruments, their sensitivity to produce correct and relevant information and the procedures for assessment of alarms and follow-up response measures.

An important condition for the successful implementation of nuclear security systems for protecting a major public event is the coverage of potential targets, to the extent possible, with adequate numbers of radiation instruments appropriately adapted to detect radiation, in accordance with procedures.

The emergency response organizations must follow **established and trained procedures**, which should include:

- i. Assessment for resolving immediate threats and responding appropriately
- ii. Roster of the response team with their responsibilities and contact information;
- iii. Means of transport for the response organization's personnel, equipment and related infrastructures;
- iv. Step by step actions to be performed by each response individual;
- v. Procedures for response to all credible scenarios;
- vi. Response reporting forms;
- vii. Equipment list and basic description of each piece of equipment;

viii. Useful references and supporting bibliography.

In the case that the situation constitutes a security event with the dispersal of radioactive material and the event escalates, appropriate **response procedures** should be applied by the designated emergency response team, such as:

- i. Site control:
 - a. Recommend isolation and/or evacuation up to radiation safety perimeter, to be determined, at the scene, by the responders;
- ii. Compound hazards assessment/scene assessment.
- iii. Apply danger reduction procedures.
- iv. Evaluate the radiological status and consequences through monitoring activities:
 - a. Dose rate;
 - b. Assessment of exposure through various pathways;
 - c. Level of protection needed.
- v. Rescue and triage operations —evacuate people, assemble in a safe area.
- vi. Public announcements and perceptions
- vii. Forensic evidence management.
- viii. Recovery operations:
 - a. Population monitoring, decontamination and registration
 - b. Medical management and biodosimetry;
 - c. Environmental remediation;
 - d. Radiological cleanup;
 - e. Embargo of zones/areas.
- ix. Restore operations — long term impacts

7.10. Step 10. Identify and Quantify vulnerabilities, determine areas for improvement, and propose upgrades

Once the previous steps have been completed, the SVA process will summarize all vulnerable points of the process to perform an in-depth VA of the public space. This covers the baseline current situation) and decides of the effectiveness of the security elements in protecting public spaces against the identified threat. If overall public space security meets determined requirements on accepted risk (step 2), then the assessment is complete. Otherwise, areas for improvement are proposed.

Within SAFE-CITIES SVA there two approaches on vulnerability quantification, which may independently provide an important considerations, but collectively describe the complete appraisal of the public space in question. However, both have a common element: **vulnerability is assessed against established security protection policies** (SVA step 2) and (SVA step 6) and the key performance parameters and indicators there.

Within SAFE-CITIES we implement two approaches for VA: **compliance and performance** based.

- **Compliance-based VA** depends on assessing the conformance to specified policies or regulations either defined through respective legislative and / or regulatory documents and internally established policies and goals. It is mainly based on metrics for analysing the presence of the specified equipment – personnel and procedures.
- **Performance-based** approaches evaluate how each element of the public space security system operates and contributes to overall system effectiveness. This way the dynamics of the adversary and protective actions are taken into account.

The use of compliance-based VA is highly effective against low risks and are suited for cost-benefit analyses documenting those protective measures which are not the most cost-effective risk management option. A compliance-based analysis is easier to perform because the measure of system effectiveness could be easily defined factors: e.g. the presence of prescribed security systems, equipment, procedures, and people.

The analysis consists of a review of facility conformance to the compliance requirements, and the use of checklists to document the presence or absence of components, and a deficiency report (SVA step 12) that notes where the facility is out of compliance. Typical vulnerabilities include weak door locks, the absence of guards, poor password controls, and insufficient distance between a building and a street. Assessing of weak / vulnerable elements of the public space can include the following elements:

- **Structural and design** issues which examples include: a) poor perimeter fencing with holes, gaps, vegetation overgrowth, etc., b) building design with floor plans that inhibit access control measures, ground floor windows along a heavy pedestrian route, etc., c) tunnels and drains that permit an avenue of approach by an adversary, d) unsecured doors that allow uncontrolled access, e) parking lots provide adversaries with a venue for observing a facility, perpetrating a crime, detonating mobile explosive devices, etc. f) vehicle barriers that are not reinforced and appropriate, g) untrained guard forces h) Unsecured windows and i) insufficient access control that allows adversaries a potential means of entry either detected or undetected and many more.
- **Technical, operational and support equipment**, that allow for a) signal interceptions that can occur when using devices like cell phones, wireless networked computers, and personal digital assistants (PDAs), b) control of compromising emanations from telecommunications and information systems equipment, c) equipment tampering in which equipment is modified to permit collection of information by an adversary and d) remote activation/operation that allows modifications or programming permitting an adversary to remotely activate and/or operate equipment.

- **Organizational / Decision making** process that could be linked to a) poor practices that potentially place critical assets at risk. For example, failure to develop and operate a property control system, b) observable practices, activities, or assets that can be surveilled. The information gained could be utilized to threaten critical assets, c) Operations Security (OPSEC) issues deficiencies – the lack of an analytical process used to deny an adversary information, generally unclassified, concerning an organization's intentions and capabilities by identifying, controlling, and protecting indicators associated with planning processes or operations.
- **Human factors & security culture** that may include a) big ego: Persons with a big ego may mishandle or improperly protect critical assets, b) Anger management problems: Persons with anger management problems may damage or destroy critical assets out of anger, c) Are ignorant of technology: Persons who are ignorant of technology fail to learn how to properly operate computers, secure telephones, etc. d) Behavioural issues for disgruntled personnel, persons with personality disorders, etc. These persons may represent either a direct or indirect threat to assets, e) Boredom: Persons suffering from boredom may become careless. f) greedy: Persons who are greedy may compromise or steal critical assets for personal gain, g) Overworked: Persons who are overworked may become careless etc.

The SVA team reviews baseline system effectiveness and makes a determination of the effectiveness of the security system elements in protecting targets against the DBT/examined threat. If overall system effectiveness or VA meets the determined requirement, then the assessment is complete.

Performance-based analysis can use either qualitative or quantitative techniques, building on the implementation of the scenario building process (SVA step 8) fully introducing the public space security functions (SVA step 6). The path analysis approach described in Section 7.8.1 illustrates the paths that adversaries can follow to accomplish their goal and the perceived impacts according to the risk scenario. Through the path analysis the performance metrics of the security functions are quantified allowing the assessment of weaknesses and loopholes along all credible adversary paths into the public space measured by the probability of interruption of the attack.

The scenario-based analysis aids in determining whether the system has vulnerabilities that could be exploited by adversaries using varying tactics, (SVA step 3), as well actions from the response forces (LEAs, local police etc). Within the scenario builder, and especially the use of digital solutions as those introduced in SAFE-CITIES, it is possible to consider different scenarios (day / night, weather, social, events, policies – functions and measures, ...) in the locality and proximity of the public space.

The scenario-based approaches could also consider neutralization / detainment analyses (as described in section 7.9.1), and also laying the groundwork for the deployment of emergency responders (section 7.9.2). The public space security

system can be determined using qualitative or quantitative techniques, including probabilistic assessments of security functions (detection, interruption, ...)

Interaction with LCN

- Establish vulnerability identification committees within LCNs to regularly assess and report vulnerabilities.
- Provide LCNs with vulnerability assessment tools and templates for standardized reporting.

7.11. Step 11. Re-evaluate public space with Proposed Improvements.

In the event that the baseline VA analysis shows that the system does not meet its protection objectives (SVA step 10) then the SVA team can propose security upgrades that will address them. These upgrades should not only be concerned with technical recommendations but are also including functional improvements that can be achieved by increasing performance. Once the upgrades are planned and/or defined, a new VA should be conducted and related metrics should be determined, provided that all assumptions made are kept constant. The process is repeated until upgrades are satisfactory addressing the system vulnerabilities and are increasing the overall public space's security in an effective manner. Societal and urban planning component of the public space should also be considered (step 4).

A risk-informed, approach should be followed, (step 7), prioritizing the interventions on assets that are exposed to the highest risk levels supported by a cost-benefit analysis, resulting in a trade-off. Innovative elements of public space protection such as enhanced public – private cooperation, local citizens networks and advanced simulation capabilities should be considered

The results of the SVA could provide a considerable focus on emerging threats with higher risk level and provided the opportunity for a focused effort for the identification of the needed type of technologies to be adopted for the mitigation of these threats. The SVA should be conducted again, taking into account the proposed and postulated upgrades.

Usually a strategic approach to risk reduction involves the following factors:

- Assessment of risk: based on the SVA process
- Prioritization of threats/assets: What threats expose the greatest vulnerability and can be reduced with countermeasures?
- Acceptance of risk: What risks cannot be realistically reduced or are too remote to call for significant countermeasures?

- Adoption of efficient and sensitive risk-reduction strategies: What is the proper balance between reduction of risk and the everyday use of the site? What is the cost and benefit of each risk-reduction strategy?
- Improving security strategies of public spaces
- Elaboration/enhancement of the security strategy including innovative insights into the identified soft targets to better focus on their mitigating actions.
- Better preparation and cooperation with stakeholders

Interaction with LCN

- Engage LCNs in urban planning discussions to ensure proposed improvements align with community needs.
- Use online surveys to gather community input on proposed changes.

7.12. Step 12. Reporting, Training and Risk Communication actions

The final step of the SVA is reporting the results in a manner useable to the responsible decision-makers. The goal of the reporting phase is to provide accurate unbiased information that clearly and in details defines the current security effectiveness and provides potential solutions in case of system's ineffectiveness.

Additionally the SVA team could provide training related to the implementation of the security measures (SAFE – CTIES D4.4 provides such training materials and also engage in risk communication process to the wider local communities and specialised security subject matter experts.

Interaction with LCN

- Create accessible and transparent reports that summarize results and recommendations for LCNs.
- Develop user-friendly formats, such as video summaries and infographics, to ensure clear communication.

8. SAFE-CITIES SVA Quantification

The following sections describes an initial set of indicators that can be used to provide quantifiable metrics and support the SVA process. The project team can select the most pertinent indicators and provide informed categorization based on historical data, expert opinions and literature review.

Table 16: Table of SVA related indicators.

SVA indicators	Details
Human factors	Composition of participants, important people, organizers, event management personnel ability
Management and prevention factors	Guarantee for the security operation of public space including the relevant schemes and technical means, SVA assessments
Site and equipment factors	Site / equipment condition, daily management and maintenance of the equipment, and the equipment usage optimization.
Risk factors	Domestic and foreign political situation, type and nature of event, social situation and attention of event
PPS effectiveness	Probability of interruption of attack * probability of neutralization of the adversary
Security factors	Security of public space, Behaviour score on security classification for access control, response measures (permanent and ad hoc)
Building factors	Ownership and importance, clustering and proximity to iconic / symbolic buildings
Policy factors	Level of cross- and within institutional coordination, dominant policy, budgetary issues
Response factors	Countermeasures tested, incident response time, communication chain and effectiveness

9. SVA testing and evaluation protocol

A proper SVA framework should be linked with suitable testing and evaluation protocols in order to a) assess their correctness and robustness, b) improve the data collection process for future SVA and c) develop, and update emergency response and security upgrade action plans, programs, policies and procedures. The following types could be considered:

- **Multidisciplinary workshops** with the participation of related stakeholders (depending on the case), responsible for the protection of public spaces. The workshops provide a good opportunity for the generation of ideas, information sharing, exchange of good practices and raising the stakeholder's risk awareness. Moreover, the interaction can contribute towards a common language and common risk understanding and communication.
- **Discussion-based exercise**, requires little resources and can be handled internally and does not disrupt or interrupt the public space daily routine
- **Practical exercise** that requires major resources and more planning (also involve external actors). However, it can identify problems in security measures implemented. All employees have the opportunity to practice their roles. Practical exercises can create confidence that real events or incidents can be handled.
- **Public Space Tabletop Exercises** should be designed and implemented to assist the stakeholders by leveraging on existing knowledge and SVA results and be flexibly tailored to their specific needs. A main recommendation of the public space community would be to prepare templates and examples

The developed SVA will be initially tested in all pilot sites against multiple threat scenarios to (a) demonstrate its validity and acceptance by the project's stakeholders, (b) collect reference data in support of the development of the SAFE-CITIES platform.

10. SVA integration within SAFE-CITIES software

The data requirements and software for implementing the SVA have been discussed in D2.1. However and in order to facilitate the implementation of the SVA the consortium decided to **move beyond the GA and introduce MAESTRO's latest feature the Security Vulnerability Assessment (SVA) tool**, that offers a practical way to examine the safety of public spaces. It provides an in-depth analysis of potential risks, the severity of possible incidents, and the attractiveness of the area to potential threats.

The first step of the SVA tool is to first select a particular public space to assess. This targeted method ensures that the analysis is relevant and informative, giving you insights specific to that location's security issues. The next step is to answer all the wizard's questions (described in SVA steps 3 / 6 / 7), leading to the assessment of the place of interest. These questions cover the likelihood, risk, impact and attractiveness of threats and whether the chosen public space might be a target, giving you a well-rounded view of any vulnerabilities.

Based user's input, the SVA calculates the level of risk, potential impact, and the area's attractiveness for threats and the results are presented visually on the map (SVA step 1-7). The area of interest is color-coded to show risk levels at a glance, from green (low risk) to red (high risk), with a corresponding scale from 1 to 5. This visual aid is a quick reference that helps in making informed decisions to improve the area's safety. In the forthcoming period this tool will be linked to the SAFE-CITIES scenario builder.

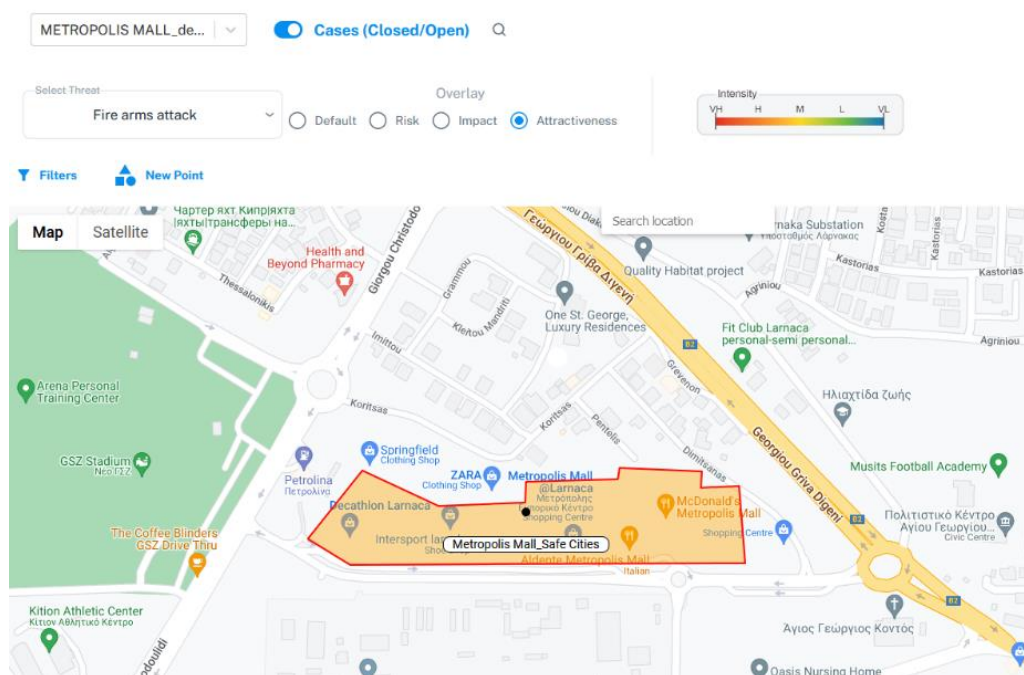


Figure 14: Results screenshot for Attractiveness.

11. Conclusions

This Deliverable introduced the revised SAFE-CITIES security and vulnerability assessment framework, following a comprehensive development process that included workshops and interaction with the project partners benefiting from the pluralism and diversity of expertise.

The revised version has managed to capture new trends to the public security domain, being aligned with EU policies and recommendations and bringing new insights on how to conduct public space SVA. In this perspective the consortium developed the MAESTRO SVA tool to support the proposed process.

The revised SAFE-CITIES SVA Framework introduces elements of “secure city by design” in the characterization of the public space using the ATLAS tools (Task 2.3), a parsimonious “citizen engagement” strategy supported by engagement tools (presented in D2.3) and a consolidated framework and recommendations for enhancing public-private cooperation. It reports the outputs from T2.3, T2.4 and T2.5.

12. References

- European Commission (2022), Security by Design: Protection of public spaces from terrorist attacks.
- United Nations Office of counter-terrorism (2022), Protecting urban centres from terrorist attacks – Good practices guide, Module 2, Global Programme on Countering Terrorist Threats against Vulnerable Targets.
- Al-Ghiyadh, M. A-K., Al-Khafaji, S.J. N. (2021), "The Role of Urban Planning and Urban Design on Safe Cities", 2021 IOP Conf. Series: Materials Science and Engineering 1058 012065.
- Coppola, F., Grimaldi, M., Fasolino, I. (eds.) (2021), Safe urban space. Strategies and actions for an integrated approach to settlement quality, Federico II University Press, Naples.
- Gehl - Making Cities for People (2022), Public Space and Public Life during COVID-19.
- Bolici, R., Gambaro, M. (2020), "La sicurezza urbana per la qualità dello spazio pubblico", *TECHNE* 19, pp. 104-113.
- Perspective.brussels, Department Territorial Strategy (2019, October), Guide to the integration of security systems in public spaces, Brussels-Capital Region.
- The Nordic Council of Ministers (2017), The nordic safe cities guide. Insights, inspiration and best practice for your city.
- Home Office of Great Britain (2012, January), Protecting Crowded Places: Design and Technical Issues.
- The Global Cultural Districts Network - GCDN (2012, January), Beyond Concrete Barriers. Innovation in Urban Furniture and Security in Public Space.
- Cardia, C., Bottigelli, C. (2011), Progettare la città sicura. Pianificazione, disegno urbano e gestione degli spazi pubblici. Hoepli, Milan.
- Politecnico di Milano, Laboratorio qualità urbana e sicurezza (eds.) (2006-2007), Pianificazione, disegno urbano, gestione degli spazi per la sicurezza, Manuale, AGIS – Action SAFEPOLIS.
- Nadel, B. A. (2004), Building security: Handbook for architectural planning and design. McGraw Hill Professional, New York.
- Jeffery, C.R. (1971), Crime Prevention Through Environmental Design. Sage Publications, Beverly Hills.
- JRC (2023), Karlos, V. and Larcher, M., Protection Against Unmanned Aircraft Systems – Handbook on UAS risk assessment and principles for physical hardening of buildings and sites, Joint Research Centre, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/969680, JRC132967
- IAEA (2012). Nuclear security systems and measures for major public events: implementing guide. — Vienna: International Atomic Energy Agency, 2012. ISBN 978-92-0-127010-8

13. Appendix 1 – Existing good practices on public private partnerships in the field of public space protection

For the protection of public spaces, CoESS recommends as good practice a model of a “Security Continuum” between operators, law enforcement, and private security. Good practices for such public-private collaboration exist at national, local, and location-specific level. Examples that reflect multiple good practices of the European Commission’s Guide include:

National level

Spain: For almost a decade LEAs have established cooperation programmes with the private security sector in their respective competence area, e.g. Red Azul at the Policia Nacional and Programa Coopera at the Guardia Civil, all based on mutual exchange of information and reciprocity. Similar programmes exist at the level of the Basque and Catalan Police Forces.

The Red Azul Programme between the Spanish National Police and private security was launched in 2012 and establishes a model of professional collaboration of complementarity and co-responsibility, aiming at the pooling of resources, collaborative operational planning and the integration of information from private security into the intelligence system of the National Police. It transcends the current model of legal requirements and moves from the situation of the mere use of private security resources by LEA to a scenario of sharing of resources that imply the establishment of a true “security alliance” between private security and the National Police.

In its collaborative relationship with the Private Security Sector, the National Police assumes the following commitments:

- Reciprocity: On the part of the National Police and depending on the degree of relationship achieved in the collaboration (see further below), reciprocal information exchange and support will be provided as to what is necessary at all times for the efficient fulfilment of the functions assigned to the private security services.
- Integration and distribution of information: The information from private security will be integrated into the intelligence system of the National Police, for exploitation by the competent Police Units.
- Participation in planning: In the operational planning of the National Police, the active participation of the services and capabilities of the private security service will be considered.
- Continuous improvement: The National Police takes into account any proposals to improve collaboration made by the private security sector.

On the other hand, PSCs who decided to participate in the collaboration programme

with the National Police assume the following commitments:

- Use the procedures and channels provided by the National Police to carry out the different activities of collaboration.
- Make available to the National Police all information it has about criminal acts or events that may affect public security, corresponding to its area of competence.
- Comply at all times with its duty of assistance and collaboration, providing the National Police, both on its own initiative and at the Police's request, with the information and support that is necessary in the preventive and investigative areas.
- Make good use of the information received from the National Police, using it in the most appropriate way to improve citizen security and for the effectiveness and efficiency of private security service, and for the exclusive purposes for which it was requested and provided.

This collaboration fully respects what is foreseen by the legal framework in Spain, and is exclusively based on the needs in public security as well as mutual trust and loyalty.

For the exchange of information and operational support from the National Police to private security, the following elements must be met:

- The request made must be in accordance with the activity or function of the PSC and necessary for the service.
- The request must have potential or interest for public security.
- The response will be limited to participating or executing what is truly relevant and appropriate to the request made.

The information that can be provided and received by the National Police within the Red Azul Programme will refer to the communication of security incidents and alerts, special events, execution of plans, detained, identified or searched persons, stolen or suspicious vehicles, criminal modalities, evolution of crime, information bulletins, reports, background checks and others of a similar nature that may benefit public security.

The information that is provided to private security by the National Police depends on the commitment reached between the two parties. An evaluation will be carried out based on the effectiveness and commitment of the PSC demonstrated with the National Police. Within this evaluation four degrees of collaboration exist - the first being the one with the least contribution of information and the last being the most thanks to the PSCs active and constant participation.

In concrete terms, the Red Azul Collaboration is organised into four Work Programmes:

1. **MANAGE:** This programme is administrative in nature and is aimed at PSCs,

Departments and Offices. In this way, collaboration is encouraged and any operational needs or collaboration problems are mainly evaluated and detected.

2. OPERA: Operational programme, aimed essentially at business associations and unions, PSCs and Security Departments and detective offices.
3. INFORM: Communications programme aimed at the sector to provide general and specific information, depending on the area of action in question. It uses several tools to improve the distribution of information.
4. WATCH: This communication programme is aimed at private security officers and its purpose is to form a space for relationships with them. To access the programme, security officers have to enter among others their Professional Identity Card number.

With the implementation of the COOPERA Program in 2010, the Spanish Guardia Civil has been making an effort, within the scope of its powers, to optimise its public-private collaboration with the security sector. Due to the maturity of the sector in Spain, it aims to integrate the private sector services, enhance public security capabilities, define data to be exchanged, as well as other approaches to guarantee a security continuum and the effectiveness of the collaboration. The Programme can be joined voluntarily by duly registered and licensed PSCs and consists of the following:

- Formal framework: The company signs a collaboration operating procedure. Institutional contact between the Guardia Civil and PSCs will be carried out at Manager level (centralised) and operational level (provincial level).
- Exchange of contacts: When joining the Programme, PSCs will provide the contact information of the Director or Security Manager who will act as interlocutor to the LEAs at management level, but also, if applicable, regional contacts and interlocutors to establish the operational level of the programme and the appropriate communication links down to the local ground.
- Safe communication channels: the means of communication are regulated through the programme.
- Regular meeting forum: Coordinated groups meet at least twice a year at operational, and once a year at management, level. They are permanent bodies representing LEAs and PSCs, directed by the Guardia Civil, without prejudice to maintaining permanent contact.
- Information exchange: PSCs provide information on all those aspects that contribute to improve the fight against crime, for example on suspicious or criminal activities and complaints and modus operandi of criminal networkers. Specific communication channels exist for urgent cases. LEAs provide information to PSCs on facts or circumstances that may affect the safety of private security personnel or the operation of its services, such as road

closures and public order disruptions, serious criminal acts, fires and other disasters, and urgent threats. Such urgent information includes local situation reports, anti-terrorist prevention data and changes in the threat landscape, local or general protection and prevention plans, as well as operational information.

- Reporting: Joint reports are drafted by the Guardia Civil to create a common security culture while facilitating the preparation of risk analyses for entities participating in the program on aspects related to security, and crime. They are based on open sources and data exchanged.
- Joint Training: the Guardia Civil coordinates joint training with different security services, both aimed at management and operational level.

France: In 2019, the representatives of private security industry and the Ministry of Interior signed a Protocol allowing the exchange of operational information between the Interior Security and PSCs at the local level. The signatories have worked on this agreement for several months. It gives substance to the "security continuum", which French MP Alice Thourot, the rapporteur of the Parliamentary Committee on this issue, has been supporting. The document concretely aims to designate local reference contact persons and representatives of PSCs, as well as Security Directors – coordinated by the national private security industry association.

Italy: The "Mille Occhi sulla città" initiative was first launched in 2010. It is a protocol between the government (Ministry of Interior), the association of Italian communes and several private security associations. The agreement is based on the realisation that:

- Citizens' security is a common good, the protection of which requires the synergetic action of the authorities and the private sector.
- The coordination of public and private initiatives needs to be part of a "security system" governed by the principles of coordination and subsidiarity.
- There is a need to "reach the maximum level of cooperation between the authorities in charge of public security, the national police forces, as well as the local police forces and PSCs, which are a complement to the public security.

Over 50 cities across Italy have been implementing the programme since the early 2010s and this number continues to increase.

The agreement states that private security, within its activities of "complementary security", may perform duties of observation and collect information relevant and useful for the police forces in order to prevent crime. In doing this, the document specifies that the PSCs may not perform public functions. The type of information is not described in detail but pertains to public order and security, including environmental factors that may impact urban security.

Criteria and modalities of cooperation between stakeholders are described in further

details in the agreements signed in 2010 and renewed without changes in 2013 and 2019. The contents and implementation are discussed at a “technical table”, which is also in charge of standardising procedures and technologies for the communication of information. The “technical table” is coordinated by the Central Directorate of Criminal Police.

The security officers, where relevant, may join police training programmes in order to perform their information collection and reporting.

The programme is monitored and evaluated by the authorities and proposals are made for its improvement, which are discussed by the public and private stakeholders.

Operational characteristics: police control rooms dispatch relevant information to private security control rooms, so that these can alert the respective patrols, and thereby increase the number of operators able to monitor situations. This is subject to the information not being under secrecy or operational restriction, and compliant with GDPR rules.

Examples of information exchanged include:

- Suspicious vehicles or persons.
- Possible escapes from crime scenes.
- Theft of vehicles.
- Assistance to people: children, older or confused people or people requiring assistance.
- Presence of obstacles on roads or tracks.
- Interruption of deliveries of sources of energy.
- Any other situation arising suspicion that a crime is about to be committed.
- Significant urban degradation or social unrest.

Local level

City of Oslo/Norway: The “Sentrum” model in Oslo has developed different areas for cooperation between the police, security industry, public sector participants and voluntary organisations, including a security guard meeting and special analysis forms reporting on criminal activity and incidents. Public spaces where this public-private collaboration is active include shopping centres and other urban environments.

Experience shows that the Sentrum model has helped to establish an open and honest dialogue between the participants.

The special analysis forms, to be regularly completed by all actors' intelligence, have helped to increase the understanding of knowledge-based strategies and target-

oriented management. The security guard meetings lower the threshold for contact and increase each party's understanding of the others' role and functions.

The security guard meeting takes place once a week between the police and PSCs at the Sentrum police station. Personnel from the police at Sentrum and Grønland police stations participate, along with personnel from various departments, depending on incidents or current criminal cases. The police are responsible for leading the security guard meetings and for taking minutes, which are distributed to all the participants after each meeting. The analysis and intelligence forms are used by the PSCs. Each PSC submits the form latest the day before the meeting. The information is reviewed by the police prior to the meeting and discussed either at the plenary meeting or at a separate meeting with the relevant PSC, as necessary. The special analysis forms, to be regularly completed by all actors' intelligence, have helped to increase the understanding of knowledge-based strategies and target-oriented management. The security guard meetings lower the threshold for contact and increase each party's understanding of the others' role and functions.

The success criteria have been:

- The police are responsible for holding and guiding the meetings.
- Fixed weekly meetings.
- The participants submit their forms prior to the meeting.
- Follow-up of cases and evaluation of incidents.
- Participants are at management level.

Municipalities of Mechelen-Willebroek/Belgium:

Municipalities of Mechelen-Willebroek/Belgium: Since the new Belgian private security law was adopted in 2017, local authorities can rely more on security companies – e.g. as their competencies and tasks in public spaces are now much clearer defined. And municipalities such as those of Mechelen and Willebroek make use of this opportunity. Both municipalities were subject to high crime rates since the 1990s and therefore developed a comprehensive public security action plan, which is described in detail in (Cools, Mark (2018)) and which includes enhanced public-private collaboration.

For example, consortium surveillance in the Mechelen industrial zone is an example of successful cooperation between the police and the private security sector. Services provided by private security in the zone, determined by a temporary contract, include:

- Perimeter control, including the permanent presence of a security officer as well as access / exit control;
- mobile patrols or movements in the industrial zone;

- mobile intervention after alarm.

In the set-up, several partners are involved, including multiple security companies, the police, industrial zones and the government on the basis of a municipal cooperation protocol. Consortium monitoring is also cost-efficient because several companies share the financial burden. Similar public-private collaboration initiatives exist in Belgium, but the Mechelen-Willebroek municipalities were the first ones to implement it. In the collaboration framework, security companies are required to report daily to the police. With the new private security law in Belgium, such frameworks can also be applied in other zones such as shopping areas.

To this end, a dedicated research conducted by Prof Dr Mark Cools from the University of Gent³⁹ looked into which other tasks of the urban/municipal security policy in Mechelen-Willebroek can be delegated on behalf of law enforcement to the security sector. The respective research comes to the following conclusions:

The takeover of public tasks by security services cannot and should not be mistaken for privatization in itself, but should be interpreted as a supporting subcontracting where the local police by definition retains and must maintain direction and control.

Advantages of public-private collaboration for the protection of public spaces include (1) freeing-up policy capacity to law enforcement core tasks; (2) specialization of the private security sector in certain tasks; (3) investment of security companies into the use and management of innovative security solutions; (4) mandatory training set by legislation ensures a continuous investment within the security companies into officers; (5) the diversity of the private security sector representing society itself which supports visibility and synergy with citizens; and (6) long-established experience of the security industry in collaborating with the police.

Tasks identified by the research which can be delegated to private security include:

- Public perimeter surveillance.
- Providing criminal intelligence in the public spaces.
- Supporting public order through event security, surveillance of public spaces (incl. crime hot spots), city patrol guarding.

Important factors for this public-private collaboration to work include as per the study:

- Sectoral regulation which clearly defines tasks and competencies of private security in public spaces.
- Joint trust-building within law enforcement and security services.
- Frameworks for cumulative information exchange, networking and collaboration.

³⁹ Cools, Mark (2018): Private veiligheid in een stedelijke en gemeentelijke context

- Lead role of the local security authorities (mayor, chief of police), also through issuing clear guidance in advance, and involvement of the security companies' management.

City of Palma de Mallorca/Spain⁴⁰: Public-private collaboration is a very common way of protecting public spaces in Spain, so numerous examples can be found in the country.

For example, the Spanish city of Palma de Mallorca engaged in a temporary public-private collaboration for the year of 2020 with private security services to secure the organisation of public events such as Nadal i Reis, Nadal i Reis, and Estiu, providing services such as:

- Access control in public spaces, but also those with restricted public access (such as stages, etc.), including specific arrangements for people with disabilities.
- Surveillance of the public spaces.
- Prevention of delinquent and/or criminal behaviour, as well as reporting to LEA in case of an incident.
- Work with LEAs on the organisation and execution of emergency and security plans.
- Reporting and analysis after each event on criminal activity and incidents.

In the exercise of their duties and in situations of need, the security officers followed the instructions given by forces of LEAs, including fire brigades, civil protection, and health services. The tenders of public procurers thereby included clear selection criteria for the service provider, including compliance with law and collective agreements, adequate insurance policies covering civil liability for the duration of the contract, appropriate training and qualification of staff (including refresher courses)

The public-private collaboration was organised through a clear point of contact and technical coordinator as head of surveillance at the responsible PSC. This person was responsible for giving the orders or work instructions to the rest of the security staff and coordinated the work with the municipal services involved with the organisation of the festivities. This person had to be present at the meetings convened by the Palma City Council in order to guarantee a collaboration on the implementation of security plans, and also to provide proposals for improvements and additional measures for enhanced security by the private sector.


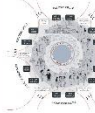
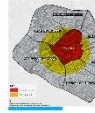







Port of Rotterdam/the Netherlands: The project "Oog en Oor" in the Seaport of Rotterdam is a cooperation between the Seaport Police and two security companies.

⁴⁰<https://contrataciondelestado.es/wps/wcm/connect/67e5d7ed-82ae-4fa9-ac95-616b006f1982/DOC2019112011243103+Plec+de+prescripciones+tecnicas.pdf?MOD=AJPERES>

It set up a common real-time information exchange between the partners in the security chain. The type of information from the police side the information is about suspicious vehicles, goods, people, pictures, and modus operandi of which security companies should be aware in order to protect the port environment. From the security company's side, they report observations that are relevant to the police. The information is exchanged on an internet platform that was specifically set up for this project. The number of "eyes and ears" in the port area has hence been significantly increased, and feedback from the actors confirms the establishment of a real security culture among all stakeholders.

14. Appendix 2 – Atlas 4 safe public spaces design guiding framework

ATLAS – 4 SAFE PUBLIC SPACE DESIGN - guiding framework

	Ambitions	Recommendations	Guiding questions	
METHODOLOGICAL APPROACH How to tackle a security/safety project	>> Avoid oversensitivity to risk	Ensure proportionality between measures and potential risks Ensure balance between safety/protection and open nature of public areas/openness	Does the design promote natural surveillance, allowing people to observe and have a clear perception of the space?	Insights from design examples  Be Secure - Feel Secure (BSFS) - Enhancing community trust & well-being in Piraeus, Greece (2020-2022) The project represents a useful example of the emphasis on not just the physical aspects of security but also the social dynamics of urban life. The project places great importance on enhancing community cohesion and connectivity at the neighbourhood level. By nurturing these social bonds and networks, BSFS reinforces the fabric of the community, making it more resilient against crime.  Horizon 2020 ROCK Project (2017-2020) The ROCK Bologna Transformative Initiative lay in its participatory approach. The city sought not just to make public spaces accessible but to ensure they were inclusive open to all, and designed with the needs and insights of the community at the forefront. Over this period, the city co-ordinated with 57 diverse local actors, including five groups of disability experts, to implement its ambitious program. One of the results of the project was a collaboratively designed app for guiding the orientation.  Birmingham's Big City Plan, Birmingham, UK (2013) The Big City Plan experience stands out as a compelling reference point for urban planning due to its robust and evidence-based approach. This approach forms the very backbone of the plan, emphasizing the importance of data-driven decision-making, what makes this case even more valuable is the structure of the plan itself, which is meticulously designed to provide a clear roadmap for addressing a wide range of issues affecting the urban environment [...].  The Superblock Model (Superilla), Barcelona, Spain (2016 - ongoing) This approach represents good practice that favours and integrates safety, sustainable mobility, citizens engagement, accessibility for everybody. Streets should have carless parking, with ridged paving and long blocks in different colours for the safety and orientation of people with visual impairment, enhancement of the character of urban fabric, a reduction of pollution, biodiversity, integration of different security measures and urban furniture enabling multifunctionality and an increase in social use of public spaces and natural surveillance.  Street art programme, Milan, Italy (2016) The intervention represents a useful example of how to mitigate and "polish" the impact of these functional elements for the protection of public space, making them - albeit as a temporary solution - more suitable to the quality, social life and enjoyment of public space.  Superkilen linear urban park, Copenhagen, Denmark (2012) The intervention integrates various aspects that affect the safe design of a quality urban space: the use of different furnishing systems to protect the edges and accesses, equipment that encourages multiple uses of the space and in different time slots, the involvement of citizens in the design process, the integration of spaces for recreation and cycle/pedestrian connection networks, the creation of a physical and social link with the neighbourhood.  Triumfalnaya Square, Moscow, Russia (2014 - 2015) The square recognizes its natural vocation as a public space, meeting socialization and transit through the integration of different urban furniture (benches, bollards, trees, greenery, etc.) devices that also function as protection systems. The design choices of the space favor the use and presence of citizens at different times of the day, so as to guarantee natural surveillance, while the edges are protected by the system of bollards, stairs and bollards which resolve the difference in height with respect to the driveway.  Christiansborg Palace security measures, Copenhagen, Denmark (2015-2019) The intervention is an example of strong security architecture and landscaping in public spaces of high and social quality, capable of finding a balance between the protection of potentially sensitive spaces, historical heritage enhancement and respect and public access.  Emirates Stadium masterplan, London, UK (2006) The intervention promotes relations with the surrounding urban fabric and the creation of safe and quality public space through controlled entrances, integration of various urban protection systems and furniture and its differences in height, signage, paving, lighting, etc. which encourage the use of spaces even beyond the football matches.  Meydan Retail Complex and Multiplex, Istanbul, Turkey (2007) The intervention represents an interesting example of how the traffic system and access of a shopping center can take on the role of public space in connection with the surrounding urban context. The square is exclusively pedestrian and protected by the urban context that hosts the commercial spaces, set up with urban furniture that favour multifunctional uses.  Postdammer Platz Buildings complex masterplan, Berlin, Germany (1992 - 2000) The intervention is relevant in terms of approach to urban and architectural design. The open and covered circulation and rest areas are planned and well designed so as to separate pedestrian and vehicular flows, integrated with street furniture and green spaces. The presence of multifunctional buildings encourages the continuous use of spaces by attracting different target users (residents, workers, tourists, etc.) while keeping the area well frequented [...].
	>> Consider security measures from the early stage of design process	Avoid exclusively barrier solutions Couple with an integrated vision of 'beautiful, sustainable and inclusive' public spaces, in line with the New European Bauhaus principles	Have the security needs and expectations of the public space's users been considered and incorporated into the design process from an early stage?	
	>> Integrate existing policies	Testing/assessing the application of existing policies specifically tailored for accessibility of spaces, inclusion of vulnerable categories as surveillance, preventive design for safe spaces	Are safety and security measures designed in compliance with design-for-all principles?	
USER'S ENGAGEMENT Details concerning the involvement of stakeholders	>> Sharing processes of safety design	Create shared informed decisions-making processes following more collaborative and inclusive processes among a wider as possible stakeholder group Maintain an open and transparent process of monitoring and developing of safe spaces	How do you engage with stakeholders to understand their risk expectations and tolerance? How do you foster continuous improvement of risk assessment and management within your city?	
	>> Intersectional approach: incorporate vulnerabilities and differences	Consider different mobility impairments into the approach, Consider generational and gender approach in security by design Incorporate needs, behaviours and responses of different citizen's types into the simulations of threat scenarios	Are you communicating effectively about risk to stakeholders, ensuring they have a realistic view of potential outcomes? How are different community voices being incorporated in the design of safety measures?	
PHYSICAL INTERVENTIONS Suggestions on urban furniture and space configuration for safe places	>> Combine and integrate protection systems with a physical design of the space/area	Display the creation of barriers and boundaries protection systems according to the existing layout/asset of the space/area in order to prevent risks and threats Respect and comply with the function, social and symbolic value of space (e.g., UNESCO sites)	Do the protection systems take into consideration the urban and architectural layout of the space? Do barriers or other safety devices ensure the smooth running of activities in the space - both temporary/exceptional/seasonal (e.g., market, etc.) and daily/conventional (e.g., walking, playing, entrances, accesses, fluxes, etc.)?	
	>> Ensure the integration/balance between standardized and ad-hoc protective measures	Combine certified/standardized urban furniture for security response (e.g., benches, bollards, natural barriers, rails and fences) with other 'environmental' solutions (e.g., territoriality, natural surveillance, access control, well maintenance and management, and target hardening), as well as ad-hoc protective measures (e.g., public art)	Are the protection systems adopted all of the same type or do they integrate multiple solutions?	
	>> Consider measures enabling multifunctional uses (beyond just the security functionality)	Prefer urban furniture/ systems/solutions capable of enabling multiple uses Check if the urban furniture/ systems/solutions are compatible with the daily usability and comfort of the space (e.g., sunny and shaded areas)	Are the activities that usually take place in the space guaranteed by the solutions adopted? Do the planned urban furniture/elements serve multiple purposes (e.g., the bollards that protect the space organize areas for different uses; the barriers are useful as noticeboards or as signs, etc.)?	
	>> Consider the climate and environmental mitigation purpose/aspects in the design layout	Provide protective measures/solutions serving as climate and environmental mitigation solutions (e.g., plants, tree-lined streets, fountains, water retention devices, etc.)	Have you performed an environmental assessment of the site to identify possible vulnerabilities? Does the project have a positive contribution in terms of improving the outdoor comfort of the space?	
	>> Combine different types of security systems capable of responding to different emergencies/ attacks	Ensure the insertion of physical measures in the streetscape for specific attacks (e.g., those involving vehicles) Apply, when/if possible, general planning principles: turn areas into pedestrian routes, keep attention to access points and boundaries, identify sensitive points, identify targeted routes and access points (e.g., logistic, emergency vehicles, concentrating vehicle flows by defining protected areas, etc.) Integrate specific systems into the public space hosting public services/uses and at the same time providing/defining obstacles (e.g., furniture, topography, pavilions, etc.) Ensure integrative mechanical surveillance measure (cameras) Test the planned solutions with temporary experiments	Have you considered existing urban furniture when implementing safety measures? Have multiple and differentiated safety systems been adopted?	
References	<ul style="list-style-type: none">European Commission (2022). <i>Security by Design: Protection of public spaces from terrorist attacks</i>.United Nations Office of counter-terrorism (2022). <i>Protecting urban centres from terrorist attacks - Good practices guide, Module 2. Global Programme on Countering Terrorist Threats against Vulnerable Targets</i>.Al-Ghadyth, M. A.-K., Al-Khafaji, S.J. N. (2021). "The Role of Urban Planning and Urban Design on Safe Cities", 2021 IOP Conf. Series: Materials Science and Engineering 1058 012065.Coppola, F., Grimaldi, M., Fasolino, I. (eds.) (2021). <i>Safe urban space. Strategies and actions for an integrated approach to settlement quality</i>, Federico II University Press, Naples.Gehl - Making Cities for People (2022). <i>Public Space and Public Life during COVID-19</i>.Boldi, R., Gambaro, M. (2020). "La sicurezza urbana e la qualità dello spazio pubblico". <i>TECHNE</i> 19, pp. 104-113.Perspective.Brussels, Department Territorial Strategy (2019, October). <i>Guide to the integration of security systems in public spaces, Brussels-Capital Region</i>.The Nordic Council of Ministers (2017). <i>The nordic safe cities guide. Insights, inspiration and best practice for your city</i>.Home Office of Great Britain (2012, January). <i>Protecting Crowded Places: Design and Technical Issues</i>.The Global Cultural Districts Network - GCDN (2012, January). <i>Beyond Concrete Barriers. Innovation in Urban Furniture and Security in Public Space</i>.Cardia, C., Bottigelli, C. (2011). <i>Progettare la città sicura. Pianificazione, disegno urbano e gestione degli spazi pubblici</i>. Hoepli, Milan.Politecnico di Milano, Laboratorio qualità urbana e sicurezza (eds.) (2006-2007). <i>Pianificazione, disegno urbano, gestione degli spazi per la sicurezza</i>. Manuale AGIS - Azioni SAFEPOLIS.Nadel, B. A. (2004). <i>Building security: Handbook for architectural planning and design</i>. McGraw Hill Professional, New York.Jeffery, C.R. (1973). <i>Crime Prevention Through Environmental Design</i>. Sage Publications, Beverly Hills.			

15. Appendix 3 – Design examples portfolio

ATLAS – 4 SAFE PUBLIC SPACE DESIGN - guiding framework Design examples portfolio



Be Secure - Feel Secure (BSFS) - Enhancing community trust & well-being in Piraeus
Greece
(2020-2022)



Triumfalnaya Square
Moscow, Russia
(2014 – 2015)



Horizon 2020 ROCK Project
(2017-2020)



Christiansborg Palace security measures
Copenhagen, Denmark
(2015-2019)



Birmingham's Big City Plan
Birmingham, UK
(2013)



Emirates Stadium masterplan
London, UK
(2006)



The Superblock Model (Superilla)
Barcelona, Spain
(2016 – ongoing)



Meydan Retail Complex and Multiplex
Istanbul, Turkey
(2007)



Street art programme
Milan, Italy
(2016)

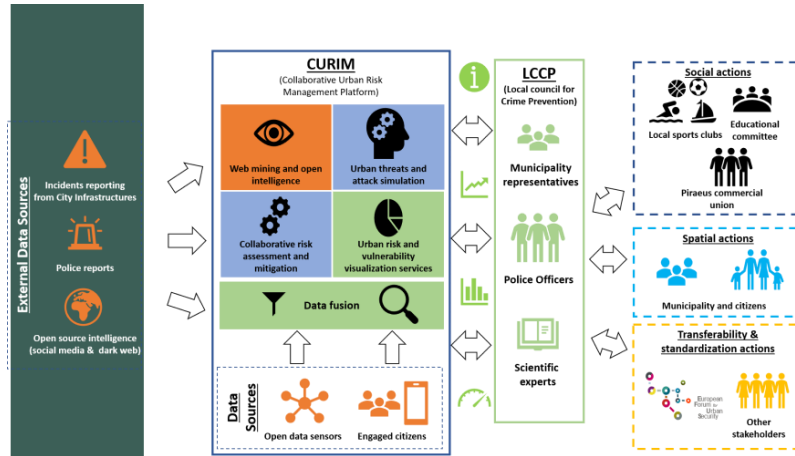


Potsdamer Platz Buildings complex masterplan
Berlin, Germany
(1992 – 2000)



Superkilen linear urban park
Copenhagen, Denmark
(2012)

Be Secure - Feel Secure (BSFS) - Enhancing community trust & well-being in Piraeus, Greece (2020-2022)



BSFS scheme.
(<https://www.bsfs-piraeus.eu/project-overview/>)

Description

The BeSecure-FeelSecure (BSFS): A Collaborative Approach to Improving Urban Security in Piraeus, Greece project aims to reinforce urban security and promote positive perception of urban safety by providing strategies & tools to link the main urban security stakeholders & facilitate their collaboration in physical-and-cyber space. BSFS will introduce the Local Council for Crime Prevention (LCCP), where the urban security city stakeholders will be represented (municipality, police, local chambers etc.) under the common goal to decide on activities and interventions that increase city resilience against crime. Under the supervision of the LCCP, BSFS will apply a number of spatial interventions, such as image management, target hardening following the CPTED "Crime Prevention through Environmental Design" model, accompanied by social activation strategies to enhance community cohesion and connectivity at neighbourhood level.

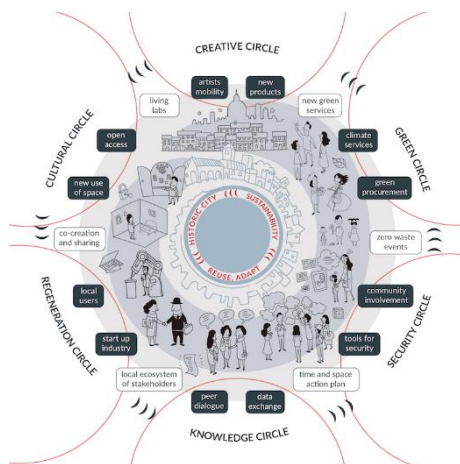
Insights for SAFE-CITIES

The project represents a useful example of the emphasis on not just the physical aspects of security but also the social dynamics of urban life. The project places great importance on enhancing community cohesion and connectivity at the neighbourhood level. By nurturing these social bonds and networks, BSFS reinforces the fabric of the community, making it more resilient against crime.

Reference/s and sources

- <https://www.bsfs-piraeus.eu/project-overview/>

Horizon 2020 ROCK Project (2017-2020)



ROCK circle

(<http://labgov.city/wp-content/uploads/sites/19/foto-cultural-herit.png>)

Description

The Rock project – Regeneration and Optimization of Cultural Heritage in Creative and Knowledge Cities – aims to regenerate, through new environmental, social, economic, and sustainable processes, several areas in the city centres of three cities: Bologna, Skopje, Lisbon. The project was ranked first in the European Horizon 2020 competition. Leading the project, which includes 32 European partners, is the Municipality of Bologna, with the University of Bologna a scientific coordinator. The project seeks to demonstrate how the historical centres of European cities can be considered living laboratories where new models of heritage-driven urban regeneration (both tangible and intangible) can be tested. It also aims to activate innovative and unconventional financing mechanisms within a circular economy framework.

The Bologna case study explores the enhancement of public spaces in the historic area using participatory processes, identifying key lessons which can be later applied to other areas and cities.

Insights for SAFE-CITIES

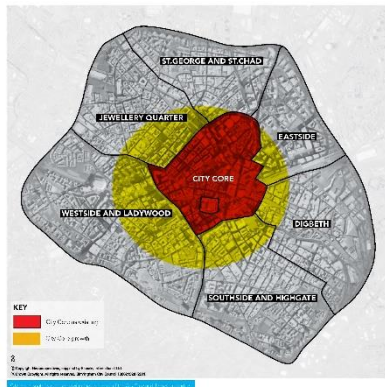
The ROCK Bologna transformative interest for SAFE CITIES lay in its participatory approach. The city sought not just to make public spaces accessible but to ensure they were inclusive, open to all, and designed with the needs and insights of the community at the forefront. Over this period, the city collaborated with 57 diverse local actors, including five groups of disability experts, to implement this ambitious program.

One of the results of the project was a collaboratively designed app for guiding the orientation of tourists and visitors in the U area.

Reference/s and sources

- <https://rockproject.eu/project>

Birmingham's Big City Plan, Birmingham, UK (2013)



Big City Plan: Boundary map

(https://www.birmingham.gov.uk/downloads/file/843/big_city_plan_boundary_map)

Description

The Big City Plan is an ambitious, far-reaching development project. The aim is to create a world-class city centre by planning for 20 years of transformation.

This comprehensive urban redevelopment plan integrates safety and security principles with a focus on creating beautiful, sustainable, and inclusive public spaces. The plan includes mixed-use development, improved transportation options, and security measures designed to be aesthetically pleasing.

The plan's focus on liveability underscores the city's commitment to not just creating accessible public spaces but also ensuring that they are truly welcoming and accommodating to all residents and visitors. It showcases the power of an inclusive approach that prioritizes the needs and experiences of the community, making it an exemplar for other cities seeking to develop more liveable and inclusive urban environments.

Insights for SAFE-CITIES

The Big City Plan experience stands out as a compelling reference point for urban planning due to its robust and evidence-based approach. This approach forms the very backbone of the plan, emphasizing the importance of data-driven decision-making. What makes this case even more valuable is the structure of the plan itself, which is meticulously designed to provide a clear roadmap for addressing a wide range of issues affecting the urban environment.

One notable aspect of this plan is its well-organized framework, featuring nested categories that delve into each relevant topic with precision. These categories offer detailed, data-based instructions and guidelines, making it a valuable resource for urban planners and policymakers looking to enhance the liveability of their areas.

Reference/s and sources

- https://www.birmingham.gov.uk/directory_record/264494/big_city_plan

The Superblock Model (Superilla), Barcelona, Spain (2016 – ongoing)



Superilla San Antoni
(<https://ajuntament.barcelona.cat/superilles/en/node/118>)

Description

Barcelona's Superblock is a flexible and replicable planning model that has been tested since 2016 in the city to configure new public spaces (green streets and squares) combining a series of interventions affecting mobility system and the introduction of safety elements to create secure and climate-friendly urban spaces.

Starting with the regular 19th-century grid designed by Ildefonso Cerdà which distinguishes the urban fabric of this Catalan city, the model defines the perimeter around a set of blocks to absorb most private and public vehicular traffic, while the inner areas are to be used exclusively by residents, pedestrians, and bicycles. Along the axes crossing these super manzanas (blocks), vehicles can travel at a maximum speed of 10 km/hr on a single reserved lane. At crossroads, car parking spaces are eliminated, and the 'freed' public space is redesigned with the insertion of new furniture, trees, and flowerbeds, outdoor terraces, and play/sports equipment. The pedestrianized areas are redesigned by architects and designers following public competitions, with the active involvement of citizens, operators, and residents. The interventions, before definitive implementation, are tested with temporary transformations of the public space.

Insights for SAFE-CITIES

This approach represents good practice that favours and integrates safety, sustainable mobility, citizen's engagement, accessibility for everybody (streets should have curbsless paving, with ridged paving and tenji blocks in different colours for the safety and orientation of people with visual impairment), enhancement of the characteristic of urban fabric, a reduction of pollution, biodiversity, integration of different security measures and urban furniture enabling multifunctionality and an increase in social use of public spaces and natural surveillance.

Reference/s and sources

- <https://ajuntament.barcelona.cat/superilles/en/>

Street art programme, Milan, Italy (2016)



Anti-terrorism barriers (new jersey),
Piazza del Duomo, Manuinvisible

(<https://www.manuinvisible.com/en/news/manu-invisible-paints-the-anti-terrorism-barriers-new-jersey-for-christmas/>)

Description

Public program created on the initiative of the Municipality of Milan as part of the 'Free Walls' project which provides street artists with 100 free walls, located in 70 areas of the city, on which artists can express themselves freely.

Among the artworks created by one of the artists involved is the decoration of some anti-terrorism barriers (new jersey) placed by the Municipality to protect some public spaces in the city of Milan (Piazza del Duomo, Piazza Fontana, and Piazza Gae Aulenti).

The works interpret and evoke the theme of peace through abstract and floral images in a period of tension and fear in frequenting large urban spaces caused by terrorism.

Insights for SAFE-CITIES

The intervention represents a useful example of how to mitigate and 'polish' the impact/presence of these functional elements for the protection of public space, making them - albeit as a temporary solution - more suitable to the quality, social life and enjoyment of public space.

Reference/s and sources

- <https://www.comune.milano.it/servizi/muri-liberi-100-muri-liberi-per-street-art>
- <https://www.manuinvisible.com/en/news/manu-invisible-paints-the-anti-terrorism-barriers-new-jersey-for-christmas/>

Superkilen linear urban park, Copenhagen, Denmark (2012)



'Black/white' part of the strip paved with asphalt and impact-resistant rubber alternating with white bands in stone
(<https://big.dk/projects/superkilen-1621>)

Description

The linear urban park - located in a semi-suburban and problematic neighbourhood of Copenhagen populated by immigrant people of different origins, is a landscape architecture and redevelopment intervention which encouraged dialogue and the comparison between the various inhabitants.

The park is divided into three parts distributed over a strip of over 750 meters characterized by different shades of colour, paving materials, topography, street furniture, green surfaces and trees. The project, designed by Topotek 1, BIG Architects and Superflex, was developed starting from a participatory process that involved the residents of the area.

Insights for SAFE-CITIES

The intervention integrates various aspects that affect the safe design of a quality urban space: the use of different furnishing systems to protect the edges and accesses, equipment that encourages multiple uses of the space and in different time slots, the involvement of citizens in the design process, the integration of spaces for rest/leisure and cycle/pedestrian connection networks, the creation of a physical and social link with the neighbourhood.

Reference/s and sources

- <https://big.dk/projects/superkilen-1621>

Christiansborg Palace security measures, Copenhagen, Denmark (2015-2019)



Christiansborg
Palace security
measures
(<https://www.lytt.dk/en/projekter/christiansborg-slotsplads>)

Description

Intervention by GHB Landscape Architects to secure and protect the borders of Christiansborg Slotsplads in Copenhagen against terrorist attacks by cars against crowds. The square is dominated by one of the fronts of the Christiansborg Palace which houses members of Parliament, politics, the Government, the Supreme Court and the Royal House of Danish parties. At the same time, many parts of Christiansborg are open to the public and the square is a frequent gathering place for pro-democracy protesters.

The square was designed as a visually calm space, dominated by an equestrian statue. The floor - largely made with reused pebbles from the previous flooring - provides an easily accessible and coherent surface where people can gather, as well as promoting a circular use of resources. Bullets of Nordic granite - the same material used for the palace's facade - stand in a circular shape on the square. The primary security element is an integrated part of the design as well as the urban space: with their smooth surface and human scale, they encourage touch and playful interaction. The formation of the string of pearls is interrupted in three points by safety bollards which guarantee access to official vehicles. The project won the Denmark Landscape Award 2019.

Insights for SAFE-CITIES

The intervention is an example of strong security architecture and peacekeeping in public space of high and sculptural quality, capable of finding a balance between the protection of potentially at-risk spaces, historical heritage enhancement/respect and public access.

Reference/s and sources

- <https://www.iflaworld.com/newsblog/winner-of-danish-landscape-architecture-award-2019-announced>

Triumfalnaya Square, Moscow, Russia (2014 – 2015)



Triumfalnaya Square

(<https://www.buromoscow.com/kopiya-triumfalnaya>)

Description

The transformation of Triumfalnaya Square in Moscow was developed following a public competition with the aim of bringing urban life back to a space mostly used for transit and car parking.

The intervention works on some main improvement actions which include: the division of the space into different areas (access borders, central space and garden); the definition of different height levels that raise the square above the road, creating protection and better use; the interpretation of the architectural characteristics of the classical language of the urban facades through a design layout with a geometric composition inspired by the gardens of the internal courtyards of the city's buildings; the improvement of the vocation of the space as a place for meeting, socializing and fun in a playful way, through the inclusion of boxes housing bars and other services, benches/swings, as well as more traditional urban furniture. The project transformed the space into a place very popular with citizens, animated by concerts, skateboarders and musicians.

Insights for SAFE-CITIES

The square reconciles its natural vocation as a public space, meeting, socialization and transit through the integration of different elements of urban furniture (seats, pavilions, trees, greenery, etc.): devices that also function as protection systems. The design choices of the space Favor the use and presence of citizens at different times of the day, so as to guarantee natural surveillance, while the edges are protected by the system of pavilions, stairs and flowerbeds which resolve the difference in height with respect to the driveway.

Reference/s and sources

- <https://www.buromoscow.com/kopiya-triumfalnaya>
- <https://www.archdaily.com/883856/triumfalnaya-square-buromoscow>

Emirates Stadium masterplan, London, UK (2006)



The Emirates Stadium in the urban context

The entrance area and the main façade
(<https://populous.com/project/emirates-stadium>)

Description

The Emirates Stadium masterplan, designed in 2006 by Populous, is located in a densely populated area of a London suburb and integrates the sports facility with housing, exhibition, commercial and event areas serving the city and the nearby neighbourhoods.

The structure creates a connection with the streets and surrounding areas, crossing the two existing railway lines with two pedestrian bridges, and introduces new public space on the raised access podium, containing the parking lot. The project also involves the wayfinding system for the entire surrounding area, so as to guide users from the car park and pedestrian passages approaching the site, to the ticket office, the hall, and the seats inside. The outdoor area is set up with concrete seats, trees, and public lighting. At the entrance to the public outdoor area, iconic large concrete letters indicate the name of the football team and protect the site which has been converted into a widely used meeting space.

Insights for SAFE-CITIES

The intervention promotes relations with the surrounding urban fabric and the creation of safe and quality public space through controlled entrances, integration of various urban protection systems and furniture (stairs and differences in height, signage, seating, lighting, etc.) which encourage the use of spaces even beyond the football matches.

Reference/s and sources

- <https://populous.com/project/emirates-stadium>

Meydan Retail Complex and Multiplex, Istanbul, Turkey (2007)



The internal courtyard/central square
(<https://architizer.com/idea/1413213/>)

Description

The Meydan Retail Complex and Multiplex is a commercial complex - designed by the Foreign Office studio, with an architectural layout and circulation system that make it a real city centre integrated into the surrounding context of one of the suburban areas of Istanbul.

The different commercial spaces are organized around a large outdoor and multifunctional urban square, located at the centre of the composition. The square is characterized by a series of pedestrian paths that connect the underground car park and is accessible and in connection with the city context by two new paths that cross the roofs of the commercial spaces, connected to the surrounding topography in several points and designed as gardens with a rich vegetation. In addition to the physical continuity between the new development and the surrounding context, skylights are introduced in the commercial areas which create visual contact between the internal and external areas, contributing to the quality of space for public use.

Insights for SAFE-CITIES

The intervention represents an interesting example of how the traffic system and access of a shopping centre can take on the role of public space in connection with the surrounding urban context. The square is exclusively pedestrian and protected by the volumes that host the commercial spaces, set up with urban furnishings that favour multifunctional uses.

Reference/s and sources

- <https://architizer.com/projects/meydan-retail-complex-and-multiplex/>

Potsdamer Platz Buildings complex masterplan, Berlin, Germany (1992 – 2000)



View of the Marlene-Dietrich-Platz public space
(<https://www.archiweb.cz/en/b/postupimske-namesti>)

Description

The Potsdamer Platz area, on the basis of a masterplan designed by the Renzo Piano Building Workshop office, has been entirely transformed into a lively, mixed-use urban centre connected with the other areas in the city to long separated by the Wall.

The masterplan respects the Berlin tradition of urban blocks and proposes a clear, compact and transparent urban design on the ground floor level (almost all the buildings have porticoes), based on the concept of the street as a public space, that connects buildings with different functional uses (offices, residences, cinemas, casinos, theatres, restaurants and shops) - created by different designers - through wide pavements and paths, squares, tree-lined avenues, water and green areas.

The pedestrian walkways and public spaces – outdoors and indoors - and the multiple possibilities of use contribute to making the neighbourhood attractive and creating a highly animated public life.

Insights for SAFE-CITIES

The intervention is relevant in terms of approach to urban and architectural design. The open and covered circulation and rest areas are protected and well designed so as to separate pedestrian and vehicular flows, integrated with street furniture and green spaces. The presence of multifunctional buildings encourages the continuous use of spaces by attracting different target users (residents, workers, tourists, etc.) while keeping the area well frequented. The glass-roofed gallery that connects some of the buildings in the complex, is an example of a commercial space protected by direct and indirect security measures, integrated with the architectural elements (multi-level galleries, transparent roofing, visual connection, etc.) and street furniture (the internal space is set up like a public pedestrian street with trees, seats, etc.).

Reference/s and sources

- <http://www.rpbw.com/project/potsdamer-platz>
- <https://www.archiweb.cz/en/b/postupimske-namesti>

16. Appendix 4 – Testing the SCPM in pilot cities

16.1. Case Study 1: Gorizia (IT) – Nova Gorica (SLO)

Within the SAFE-CITIES project, the case study of Gorizia, Italy, and Nova Gorica, Slovenia focuses on evaluating security vulnerabilities and promoting cross-border cooperation. The pre-testing of SCPM and SVA methodologies was centred on a significant cultural event, the Patti Smith Concert scheduled for October 5, 2023, near the border crossing point, organised as part of the European Capital of Culture initiative.

16.1.1. Activities Performed

Preparatory Activities (May – July 2023): Coordination meetings to initiate project activities.

Phase 1 - Assessment (03/08): Context assessment, community profile creation, stakeholder identification, and SVA adaptation.

Phase 2 - Contextualization (15/09): Implementation of SVA Steps 1-7, Phase 1 SCPM, identification of government and non-government organizations.

Phase 2 - Contextualization (22/09): Integration and validation of the community profile and identification of strategic outputs.

Phase 3 - Implementation – 4th WS October – TBD: ex-post analysis of security measures after the pre-pilot case (concert).

16.1.2. Next Steps

Ex-post analysis of security measures for the Patti Smith Concert.

Establishment of a shared calendar for LCN activities.

Conducting a participatory gap analysis for cross-border cooperation (CBC).

Application of the SVA methodology to real scenarios linked with GO2025.

Providing recommendations for enhancing the security of public spaces through cross-border cooperation.

16.2. Case Study 2: Larnaca (CY)

The case study of Larnaca, Cyprus, aims to assess security vulnerabilities and engage local stakeholders, focusing on the Radisson Blu International Larnaca Marathon scheduled for November 19, 2023. This event presents an opportunity for cross-sector collaboration.

16.2.1. Activities Performed

Preparatory Activities (August 2023 - Online): Coordination meetings to initiate project activities.

Phase 1 - Assessment (24/08 – Online): Context assessment, community profile creation, stakeholder identification, and SVA adaptation.

Phase 2 - Contextualization (31/08 – Online): Integration of the community profile and Phase 1 SCPM.

Phase 3 - Implementation (Online, September - October): Preparatory workshops with LCN members.

Phase 3 - Implementation (10/10): Kick-off meeting for LCN members in Cyprus.

16.2.2. Next Steps

Ex-post analysis of security measures for the pre-pilot event.

Integration of LCN and participatory approaches for preparation of the Larnaca Marathon in 2024.

17. Appendix 5 – Compliance-Based Vulnerability Assessment

The next set of questions provide some guidelines on how to perform Compliance-based VA and introduces a set of questions that could be included in the establishment of the security functions of a public space. Each question should be accompanied with a respective answer linked to existing policies / risk tolerance levels of the public space and community.

Governance

Does the public space / event have an SVA Team to make security management decisions?

What kind of various stakeholders SVA Team is consisted of?

Planning

Does the Public Space have a Security Plan and a Security System installed?

Does a written security and safety/emergency operations plan(s) exist?

Has the Team Received Training on the plans?

Are citizens included in the training / exposed to security arrangements and emergency procedures?

Coordination with LEAs and Emergency Responders.

Does the public space have ER procedures?

Public Alerting Capabilities

Crisis Communication plans and Procedures

Is a Cyber Security Plan implemented in the Public Space?

How often those plans are reviewed/updated

Threat vector

Exchange of threat information or alerts from LEAs (criminal, terrorism, cyber)

Based on every Threat identified, how often such incidents are found in world criminal databases?

Participation in working groups and expert tasks forces

Background checks and vetting of employees

Provision of security information to employees

Procedures for bomb threats and suspicious items

Cash management controls

Characterization of the public space

Barriers with a physical design of the space

Adoption of standardized urban furniture (e.g., benches, bollards)

Partial presence of physical measures in the streetscape for vehicle born attacks

What kind of events are taking place in the Public Space?

How many events took place on average per year?

What was the average attendance of those events?

By what means people reach the Public Space?

What is the land usage around the Public Space?

What is the Public Space recognition?

What is the capacity of Public Space's parking area?

What is the number of crew staff in Public Space's parking area?

How many communications systems are operable in Public Space?

How many communication ways are available to Security staff?

How many visual information means are used in Public Space?

Public Space security system

Security team for daily security operations

Security training

Security-related inspections or screening before people gather

Security team with comms equipment, or panic alarms

Extra personnel at critical vulnerability situations

Designated posts/patrols and written post orders

Reporting of security concerns by citizens

Well-established perimeter using natural materials or fencing/walls

Natural surveillance to the outer perimeter

Separation of public and private spaces

Fence / Purpose

Gates

Lights at perimeter

Are vehicles parked monitored

Control of vehicular parking and circulation onsite

High-speed avenue(s) on approach

Minimum stand-off distance to public space

Parking (and walkways) areas illuminated

Screening persons, bags/ packages, or deliveries

Gates/Doors closed to prevent unauthorized access

Doors be easily closed and locked to prevent access

Key control program or defined process for card access

Construction of exterior doors and windows deter or delay an attack

Some type of intrusion detection system /alarm system in place

Interior layout provides escape routes for effective emergency exits

Easy access to multiple exits

CCTV

Effective combination of camera types

Monitoring System in place

Information recorded and reviewed

Overall condition of CCTV

Protection of Computer Systems + Digital Information Protection of Computer Systems
+ Digital Information + Network Infrastructure

What Cyber Security technologies include of?

Could Public Space's SCADA Systems be identified through Internet?

How often Public Space SCADA's passwords are changing?

Purchasing a SCADA System, do you investigate if it is subjected to a zero-day vulnerabilities?

What is a common practice, to purchase a commercial off-the-shelf SCADA System or a tailor made one?

Do third party vendors/equipment suppliers have the ability for remote access to Public Space Equipment? (e.g. updating a software)

Does Cyber Security protocols prohibit plugging into Public Space's network USB flash drives/removable media devices?

USB flash drives/removable media devices must run a viroous scan, prior plugged into a network system.

Is Cyber Security investment a priority for the Public Space Management?

Were any complaints between Public Space staff that Cyber Security guidelines implemented on site were badly written, unclear and making no sense?

How often a Cyber Security awareness training is taking place for Public Space's staff?

Interruption

Likelihood that Guards and Response Forces can prevent a threat from completing a theft or a sabotage, as a result of interruption of the given malicious act.

Likelihood for the successful arrival of the Guards and Response Force at an appropriate location in time to stop the adversary,

Initial locations of response personnel

Deployment plans

Response tactics

Tactical decision making

Command and control

Does a 24-hour guarding service and Response Forces is implemented in Public Space?

Are Guards conduct random patrols in the Public Space?

Is any Alarm equipment, alarm communication paths, uninterruptible power supply and tamper protected in Guards post in Public Space?

Is a dedicated, redundant, secure and diverse transmission system for two way voice communication between the Guards post and the RF?

Is an Evaluation program conducted, (including performance testing, of the physical protection measures and of the physical protection system, including timely response of the Guards and RF), to determine reliability and effectiveness against the threat?

During the Evaluation program were any problems in- cooperation between Guards and RF?

According the DBT, are Rf numbers enough for overwhelming against adversaries?