PROJECT FINAL REPORT

Grant Agreement number: 242497

Project acronym: **RIBS**

Project title: **RESILIENT INFRASTRUCTURE AND BUILDING SECURITY**

Funding Scheme: **FP7 COLLABORATIVE PROJECT**

Period covered: **from** **1ST NOVEMBER 2010** **to** **31ST OCTOBER 2013**

Name of the scientific representative of the project's co-ordinator[1], Title and Organisation:

DR HERVE BORRION, UNIVERSITY COLLEGE LONDON

Tel: +44(0)2031083194

Fax: -

E-mail: **h.borrion@ucl.ac.uk**

Project website address: http://www.ucl.ac.uk/jdi

[1] Usually the contact person of the coordinator as specified in Art. 8.1. of the Grant Agreement.

A. Executive Summary

In RIBS, the development of requirements and measurements for protection measures to be implemented in commercial buildings was conducted through collaborative work involving different teams of security experts and end-users.

The planned work began with the creation by the teams of architects of an infrastructure model representing a commercial building, its services, occupants and assets. The method then involved the elicitation of the objectives and constraints of a range of organisations and stakeholders, including the following departments of financial institutions in Europe: management, audit, security, procurement and customer services.

A number of scenarios were then developed to represent the operational conditions that the protection measures may face in the future. Ordinary conditions were developed through observations. Extra-ordinary conditions were developed by considering those events that could potentially arise and have an impact on the stakeholders' objectives. In particular, a number of attack scenarios were developed to represent the impact of potential terrorist threats.

As a start, terrorist plans (modus operandi and targets) were specified drawing on data about past events, trend analysis and advice from practitioners. Using the attack plans as an input, the corresponding scenarios were then generated with a greater level of details by applying two simulation methods: role-playing and object-oriented discrete event simulation (DES). In order to obtain specific information about the behaviour of the hazardous agent employed, and their impact on the ecosystem, a number of additional models were developed for specialized simulation tools.

Considering the resulting scenarios (i.e. sequence of ecosystem states) as (mis)use cases, the high-level requirements of the system were then further specified by our experts in biological, chemical and explosive protection. Several security principles were selected to achieve risk reduction, and used to specify the precise functions of every protection measures, as well as their qualities. The result (requirement specifications for systems that could deal with Intruders, Explosive, Chemical and Explosive Threats) are available in the final deliverable. These were then verified through two methods: logical verification and simulations.

The validation and dissemination of the results to the broader community provides the basis needed to (1) facilitate the development of innovations by numerous SMEs that have limited security expertise, and (2) offer a new risk-based methodology for the development of requirement and measurements for physical security systems. By integrating ethical concerns at the design stage, the RIBS project is more likely to minimize the unintended impact of security technologies across the EU, and increase public acceptability. In turn this project will have positively participated in the establishment of a vibrant security technology market in Europe.

B. Summary description of project context and objectives

1. RESILIENCE OF INFRASTRUCTURE AND BUILDING SECURITY

1.1. Background

In a global context where national interests are increasingly interrelated, the most vulnerable infrastructures in Europe, and particularly the most critical ones, are primary targets for terrorists. Attacks, carried out under a national, political, or religious banner, now strike regularly in our cities, causing deaths, damage and disruption on an unprecedented scale.

National strategies across Europe consider situational protection measures as major components of our future counter-terrorism (CT) response. In continuation with their contemporary versions, tomorrow's policies and technologies will be designed to assist law enforcement agencies in deterring and detecting offenders, and disrupting their attack plans. However, it is envisaged that their presence will progressively increase to pervade our urban environment.

Most of the CT technologies currently deployed within public spaces are concentrated at a few sites including airports, embassies and major event venues. In most cases, the implementation of security procedures has noticeably affected our behaviour, and simple items such as water bottles are now on the lists of prohibited objects. In addition, the security technologies acquired to protect us are relatively expensive, and their poor efficiency undoubtedly more widely known than their effectiveness.

In comparison, very few CT measures exist outside these highly controlled places to protect the population. Encouraged by specialized agencies, a few retail places have now adopted blast-resistant glazing. However, the large majority of commercial buildings open to the public are fitted with anti-theft measures, not CT ones. Cultural venues too are poorly equipped to prevent violent attacks. Our world-renowned museums, for example, could only take limited action to protect visitors and our precious heritage.

The cause of this unpreparedness can be found in the lack of incentives for most organisations to invest in CT equipment. The frequency of serious terrorist attacks is relatively low in comparison with the number of potential targets, making security investment difficult to justify. Furthermore the need for even more security systems in society is debatable: At a time where many European governments reduce public expenditure, it seems justified to ask whether the cost of security is too high. How much should an organisation be expected to spend on public security each year? And wouldn't the introduction of such systems bring us one step closer to the surveillance society?

To ensure that the security choices we embrace are not only effective, but also in line with our national strategies and societal values, a constructive discussion of these questions should ideally take place at all levels of society. Decision makers should be able to identify the main dimensions of the problem and weigh the alternatives carefully. At the level of an organisation, a head of security should be able to select measures

that best meet the needs of the stakeholders, including the broader public. Conversely innovative companies should be encouraged to create protection systems that receive the buy-in of local governments, potential customers, and those who may be impacted by their presence in our urban environments.

At present, it is often difficult for facility managers to find effective and affordable security products that can both protect people and support their organisations' objectives. Security systems work best under specific operational conditions, and those often conflict with employee productivity or customer comfort. Equally, very few products seem to address the many issues associated with ethics and public acceptability that so often make the headlines of newspapers in democratic societies.

There may be several causes behind the gap in our suite of protection measures. For example, the poor shared understanding that exists between the public and the communities of retailers and technologists is one of them. Fundamentally it can be argued that the lack of clearly defined needs is the first barrier to the investment required to drive scientific and technological advances:

- Faced with the need to select a protection measure, decision makers must consider multiple criteria. Without a clear understanding of those criteria it is very difficult for the security industry to propose suitable products, and for security teams to justify their procurement choices.
- Protection measures are sensitive to their environments and the threats they face. Without well-defined means of translating laboratory-based innovations into operational improvements, it is difficult for the various stakeholders to evaluate and compare different measures. Seemingly good ideas can be operationally flawed in practice, due to the poor acknowledgement of operational conditions and human factors.
- Protection measures are not independent. Implemented in a given environment, they may conflict with each other, and conflict with other systems installed for commercial purposes. Without a clear understanding of the entire ecosystem, introducing a new security measure may be ineffective or even counter-productive.

For these reasons, tomorrow's protection measures must be designed not only to reduce the theoretical risk of an attack but also with greater consideration to the needs of the public and the market. Failure to integrate those in future designs will result in many barriers affecting the demand and supply of CT products.

Successful security innovations will be those capable to operate in a niche defined by the legal, socio-cultural, ethical and commercial constraints of the end-users. However, no single organisation has the knowledge and expertise needed to accurately identify this niche:

- Many S&T small and medium enterprises (SMEs) do not have sufficient knowledge about the organisations potentially targeted, or the expertise needed to specify effective security strategies.
- Many security units protecting the private sector organisations lack the ability to ask critical questions to assess the suitability of off-the-shelf security technologies, or lack the expertise needed to inform the development of new technologies.

In order to better understand the needs that future protection measures should meet, it is essential to bring together the knowledge, skills, expertise and network of four communities of stakeholders: the public, commercial organisations, law enforcement & security units as well as science and technology innovators. To achieve this aim, the European Union commissioned, through the Framework Programme 7, a number of consortia to carry out research with the view to set clear directions for the development of new counter-terrorism measures for urban environments.

2. PROJECT AIM

2.1. Aim

In 2010, the EU funded a project to improve the **Resilience of Infrastructure and Building Security** (RIBS) by supporting the specification of requirements for effective and affordable protection measures.

Focusing on commercial buildings in an urban environment, the RIBS project was built on the idea that eliciting a set of requirements and making it available to technology developers would support the development of more satisfactory security products.

In order to achieve this aim, the RIBS consortium deployed the expertise required to accurately analyse the problem of requirements engineering, considering the various factors that could affect the quality of the results. Knowledge in business, security and crime science, laws and ethics, architecture and several areas of science and technology was used to address it.

2.2. Objectives

1. Over a period of thirty-six months, the RIBS consortium developed and adopted a multi-disciplinary approach to meet the following objectives:

- To develop a set of **requirements** for new counter-terrorism protection measures for commercial buildings; including a set of **measurements** that can be used to evaluate the level of protection offered by candidate security measures proposed to be implemented in buildings and infrastructures.

2. The tasks carried out to achieve these two objectives contributed to meeting a broader objective:

- To develop and apply a **methodological framework** that can support the development of requirements for physical security measures considering a range of constraints and objectives.

3. SCOPE

3.1. Definitions

Several elements within the ‘description of work’ (DOW) limited the scope of the project:

1. The project should prioritize existing buildings and therefore retrofitting.
2. The project should consider a range of threats, namely biological, chemical, explosives, and insider or intruder (CBE-I) agents.

Beyond these constraints, the consortium was relatively free to adjust the scope of the project as required by the security situation and the state-of-the-art at the time of starting the project.

C. Description of the main S&T results/foregrounds

4. RIBS REQUIREMENTS ENGINEERING METHOD

4.1. Background

4.1.1. Requirements

Before commissioning the development of a policy or product, organisations should explicitly communicate what is expected from designers. The need for formulating requirements also applies in the field of security where designs may take the form of security policies, security procedures or security products.

To support the development of new counter terrorism measures, the RIBS project developed a set of functional and non-functional requirements for measures to be implemented in commercial retail venues such as branches of banks.

“The functional requirements define the functional effects that the protection system to be is required to have on its environment. Non-functional requirements define constraints on the way the system-to-be should satisfy its requirements or on the way it should be developed” (Van Lamsweerde 2009).

Requirement specifications contain detailed information about a design problem, including constraints of, for example, legal, physical and managerial natures. From this perspective, protection measures can thus be seen as potential solutions proposed by designers and technology innovators to that problem.

4.1.2. Measurements

To evaluate the ‘level of goodness’ of candidate designs, specific criteria can be developed for the different requirements. For example, it is important to have a means of assessing how well a proposed system meets a requirement such as *the protection system should prevent a chemical agent present in Room A from progressing to Room B*. Measurements comprise metrics and procedures that describe how to carry out the assessment, and are generally included in the requirements specification document (IEEE 2008, ISO 2011).

4.2. Related work

4.2.1. Existing problem-solving frameworks

A number of problem solving methods exist for developing or selecting effective security measures, for example, Scanning, Analysis, Response, and Assessment (SARA) (Clarke and Eck 2003), the Security Function Framework (Ekblom 2012a, 2012b), the 13 steps by Haimes and Schneiter (1996).In addition, requirements engineering framework are also available: KAOS (Dardenne 1993), i*(Yu 1993), Tropos (Bresciani et al 2004) and Common Criteria (CCSO 2006) for the development of requirements.

4.2.2. The gap

To our knowledge there were no specific requirements engineering framework specifically constructed for CT measures specifically supporting resilience of infrastructure and building security.

1. Risk management framework such as those developed by Aven (2008), Haimes (2011) and ISO (2011) are focused on the risk assessment stage but do not provide explicit information for the development of requirements.
2. Problem solving frameworks from the field of Crime Science (e.g. SARA) are designed for community policing, and do not provide appropriate guidance for the development of CT measures.
3. The Security Function Framework (Ekblom 2012a, 2012b) is a useful design framework but the relation between risk assessment and requirements is not sufficiently detailed to offer a systematic method.
4. Detailed methods from engineering sciences such as KAOS *(Van Lamsweerde 2009)* or Common Criteria (CCSO 2006) are either not sufficiently focused on security, or too focused on information (as opposed to physical) security applications.

For this reason, the work carried out was attempting to fill in the gap between risk assessment and requirements engineering, specifically for the counter terrorism domain.

4.3. Methodological approach

In order to develop and validate the requirements to be recommended for the design of protection measures, the RIBS consortium adopted a framework that enables different disciplinary approaches to be integrated together. The framework is inspired by the MCDM process approach proposed by Roy (1990) and Belton and Stewart (2002), and consists of several stages. The next section provides an overview of the method adopted in the RIBS project. The work conducted and the results are then described in the following chapters. The structure of the document matches the structure of the methodological framework.

4.3.1. Development of system requirements

When a protection measure is proposed by a company it can be classified as:

- Feasible if it is a solution satisfying objectives, constraints, and requirements.
- Unfeasible if it is a poor solution failing to satisfy at least one of the above.

The need for protection measures typically arises from a problem or need identified within an organisation. This problem or need can be reformulated to specify the top level goals, for example ‘to increase the value of the company’ (i.e. ‘to maintain or increase the value of the assets—for a constant level of liabilities— and ‘to be able to make profit’), and combined with the context of operation to form the requirements of the organisation. These requirements can then be supplemented with additional stakeholder requirements. These stakeholders may include the company employees, regulatory bodies, customers and visitors to list just a few.

The development of systems requirements arise from the specification of stakeholder requirements within the context of interest. This involves considering the potential scenarios that may occur in a given period, selecting a strategy (identifying the events to influence-prevent or encourage), selecting a set of control principles (e.g. prevention through increasing the risk perceived by an offender), and intervention mechanisms to bring about the intended effect. The functional requirements of the protection measures can then be developed and evaluated alongside the non-functional requirements.

4.3.2. Assessment of system requirements

Carried out with varying degrees of formalism, assessment is a recurrent process that contributes to the specification, analysis, prioritization, testing and verification of requirements. For this reason, it is a critical stage of requirements development.

There are several ways in which requirements can be assessed (van Lamsweerde 2009):

- Inspections and reviews
- Animation based validation
- Formal verification

4.3.3. Validation of system requirements

The need for validation

Requirements validation should be carried out to ensure that the future control measures conform to the user needs and constraints on the system. Incomplete or untraceable requirements will potentially lead to problems with regards to user acceptance or the technical quality of the system. This is especially relevant for counter terrorism measures due to the devastating consequences of terrorist attacks that cannot be prevented. Since the evaluation criteria are related to the effect of the measures in a given period, invalidation of requirements should only consider the range of conditions under which the measures are expected to operate.

Validation method

A proposed method for the validation of requirements is through falsification. Under the principle of falsification, requirements are considered valid unless the validation panel identifies a set of conditions for which they are invalid. The method has inherent limitation in terms of completeness but it is generally easier for external reviewers to identify counter examples than identifying logical defects in the way requirements were derived.

"Validation arises by failing to identify a hypothetical measure that satisfies the detailed system requirements but not the high level requirements"

A proxy for the requirements

Since it is difficult to evaluate system requirements directly, we propose to use a proxy for this purpose: *a set of hypothetical measures that satisfy the requirements*. This approach is similar to the animation based method mentioned above.
The assessment of requirements involves evaluating whether the measures meet the stakeholder requirements. Validation arises by failing to identify a hypothetical measure that satisfies the requirements but does not meet the criteria.

Scenario based validation

The method adopted to assess the proposed requirements belongs to a group of requirements engineering methods known as scenario-based validation (Some 2005). Several of the selected criteria require an analysis over a certain period of time (e.g. 5 yrs), and are based on the range of conditions that the protection measures may face during that period. Under a scenario based approach, the values of the relevant conditions of the ecosystem are captured in a set of scenario models that represent the successive states of the ecosystem over the period considered. In the RIBS project, the attacks plans that underpinned the development of the requirements were used to specify the scope of the validation scenarios.

Simulation

Under the conditions of the scenarios, many of the model components evolve as a result of complex mechanisms. In order to contribute to the description of the scenarios, computer simulation work was required to model, for example, the dispersal of hazardous agents, and the impact of an explosion on the building structure.

Sampling

As it is generally impossible to predict accurately what conditions a security system may face—and because evaluation of the requirements for every possible eventuality is not feasible in practice—the selection of conditions is therefore conducted by sampling across the range of every considered variable.

"The scenarios capture the operational conditions that the protection measures may face during the assessment period."

Methodological procedure

1. Project context

Identifying the context of the project is the first step of the method. It involves formulating the problem and identifying the aim and scope of the project, as well as the various forces and constraints that must be taken into account when carrying out the work.

1. Background
2. Project aims
3. Scope
    i. Defining the scope of the project
        1. Functional
        2. Temporal
        3. Geographical
4. Method
    i. Selecting the method used for the project
    ii. Selecting the method used for the evaluation of the results
5. Stakeholders
    i. Identifying the main stakeholders
        1. The client
        2. The decision makers
        3. Other stakeholders
6. Ecosystem
    i. Modelling the ecosystem
        1. Logical abstraction
        2. Operational abstraction
        3. Physical abstraction
7. Assumptions and Risk
    i. Listing the assumptions used at the start of the project
    ii. Identifying the main risks and challenges, and considering further studies.
8. Studies
    i. Identifying the studies to be conducted
9. Code of Ethics
    i. Specifying the code of ethics used in the project

2. Development of the high level requirements

As with any requirements engineering project, the requirements from the stakeholders (including the decision makers) must be elicited, evaluated and specified.

.

1. Eliciting the high level requirements from the stakeholders
    i. Eliciting the stakeholder' requirements for the measures to be.
    ii. Evaluating the requirements
        - Inconsistency management
        - Requirements prioritization
    iii. Specifying the high level system requirements
    iv. Verifying the high level system requirements

3. Development of specific system requirements

The requirements related to risk mitigation are further specified here. Security experts are considered as stakeholders, and help refine the range of possible strategies, methods and intervention mechanisms that will shape the final system requirements. A scenario based approach (underpinned by a set of attack plans) is employed to support the operationalization of risk based constructs. Multiple iterations are also embedded in the process to allow the adaptation of dynamic systems to be taken into account.

1. Constructing a family of evaluation criteria for the high level system requirements
2. Selection of the list of requirements to refine.
3. Identifying relevant dependencies in the environment
    i. Identification of relations between the components of the ecosystem and the stakeholders' objectives and constraints
    ii. Identification of dependencies between the components of the ecosystem
4. Modelling ordinary scenarios relevant to those requirements
    i. Scenario modelling
        - Modelling the users' activities
        - Modelling the sub-activities
5. Modelling extraordinary scenarios relevant to those requirements
    i. Specification of initiating events
    ii. Attack plan structuring
        - Variable selection
        - Value selection
        - Plan specification
    iii. Scenario modelling
        - Modelling the users' activities
        - Modelling the decision, initiation and completion stages for each activity.
6. Carrying out a sensitivity analysis of selected activities
    i. Identifying factors of performance for selected activities
    ii. Identifying suitable values for the factors
7. Specifying aspects of the proposed strategies, control principles & mechanisms
    i. Specifying the strategy
    ii. Specifying the control principles

iii. Specifying the intervention mechanisms

8. Determining the response of the various entities, and updating the scenarios.
    i. Modelling the states of the building and physical assets
    ii. Modelling the states of the perpetrator
    iii. Modelling the states of the hazardous agent
    iv. Modelling the states of the occupants
9. Reiterating the previous steps as appropriate.
10. Estimating the consequences
    i. Damage analysis
    ii. Harm from the perspective of the decision makers
    iii. Harm from the perspective of other stakeholders
11. Comparing the different alternatives and selecting the most suitable ones.
    i. Assessing the different alternatives
    ii. Selecting suitable ones
12. Specifying the systems requirements
    i. Specifying the functional requirements
    ii. Specifying the non-functional requirements
13. Internally verifying the systems requirements.

4. Simulation-based evaluation of requirements

In the fourth stage, the requirements are evaluated using the same attack plans as in the development stage. Alternative are assessed against a set of criteria derived from the high level requirements.

1. Construction of a family of criteria for the hypothetical measures
2. Development of alternatives (hypothetical measures)
3. Development of families of scenarios
    i. Modelling ordinary scenarios relevant to those requirements
    ii. Modelling extraordinary scenarios relevant to those requirements
4. Assessment of alternatives (hypothetical measures) and problem parameters
5. Iteration (5.2)

5. Validation and dissemination

In the final stage, the requirements are verified, validated and disseminated.

1. Review
2. Verification
3. Validation
4. Dissemination

5. OTHER AREAS OF PROGRESS BEYOND THE STATE OF THE ART

In order to develop and implement the methodology, the RIBS consortium contributed to the advancement of the different fields through concrete developments:

5.1. Biological protection

1. A literature review has been prepared that discussed how bioagents may be spread through an indoor environment following an attack due to the behaviours and characteristics of the building population, in terms of their typical behaviour, as well as any emergency response measures they implement.
2. A literature review of existing risk assessment methodologies has been prepared describing the existing methods of evaluating the resilience of a building to a bioattack has been produced, describing the limitations of existing methods. A novel framework for classifying protection measures has been proposed, while a fault tree analysis has been developed based on the framework components that describe the relationship between the protection measures.
3. A highly-detailed model building was constructed using the software CONTAM, and the performance characteristics of different protection measures researched and integrated into the model. This model is capable of evaluating their performance under a range of different attack scenarios, informing the relative effectiveness of the protection measures within the building, and can be used to populate the failure diagram proposed.
4. A novel laboratory research investigating the persistence and viability of microorganisms has been developed. The team has also tested the efficacy of a number of antimicrobial decontamination strategies.
5. The research has found that the persistence of microorganisms in the air was species dependant, with Gram positive organisms, such as Bacillus spp., persisting for longer. The team has also investigated the persistence of both bacterial and viral pathogens on surfaces, such as tiles. It was shown that the organisms persisted for longer than previously thought, beyond two months. These experiments were carried out using model pathogenic organisms: Staphylococcus aureus, Klebsiella pneumonia, and Adenovirus.
6. Research investigating the efficacy of a commercially available portable air cleaning device based on the use of a filter system and UV light showed that the device was effective in a small volume, however it had little effect on the viability of microorganisms in generic sized room (e.g. 40 m3). This research informed some of the BWA protection measures proposed by the RIBS team. Another device tested was one that employed hydrogen peroxide vapour to decontaminate spaces retrospectively. The research performed showed the device to be very effective against a number of pathogens, including bacterial and viral ones. Again, this work has contributed to the BWA protection measures proposed.
7. Development of requirements including different HVAC configuration, coated surfaces, air dilution and decontamination system as protection measures.

5.2. Explosive protection

1. Numerical simulations with various venting configurations were conducted by carrying out parameterization of the total area of vent. Variable degrees/locations of venting were tested and not just the extreme cases of vented vs. unvented.
2. The distribution of internal blast loading on both directions of the ceiling of a closed space was obtained from the numerical simulations that were conducted. The distribution was used in order to evaluate and clarify the limited theoretic blast load distributions that are already available in bibliography.
3. Comparative numerical simulations were conducted in order to research the impact of venting through staircase openings and in contrast to the traditional just side opening approach.
4. The significance of roof venting panels and partial high wall vented panels was tested by simulation.
5. Identification of development requirements for the simulation and wide application of FRPs for bomb blast protection of buildings.
6. These were based on the range of different types of simulations conducted, including internal, external detonations as well as large, small, contact, distant, surface and air detonations for rigid and flexible (blast-structure interaction) building models. These were compared and validated against analytical methods. The capabilities of the software proved to be adequate for the blast analysis and the design of protection measures of any real building case.
7. Evaluation of the available methods for explosion modelling existing in ANSYS/AUTODYN, including filling Euler cells with explosive material, and identification of their limitations and applicability.

5.3. Chemical protection

A comprehensive system approach comprising of a network of sensors connected to a computer with software that is capable of analysing the signals received from the sensors and taking appropriate action using protection measures such as:

1. Partition doors that automatically separate the area in which a chemical attack was detected from other zones of the building, thus preventing the attack from impacting most of the building occupants. This measure is an adaptation of fire doors used to seal areas in buildings that caught fire and prevent the heat, smoke and flames from entering areas that were not affected. Other types of sliding doors will resemble measures used to protect submarines from sinking when seawater starts penetrating some area of the vessel.
2. Automatic shutdown of airflow through the AC ducts, thus preventing the chemical materials from spreading throughout the building. This measure is an adaptation of similar measures used in fire protection systems.
3. Automatic reversal of airflow in the AC system, thus sucking the chemical materials out of the building. This measure may be extended to include some filters on the roof of the site – air suspected as contaminated will flow through this filters only when the emergency air reversal mechanism is activated.

4. Automatic opening of windows and doors, enabling free entrance of fresh air that mitigates the effect of chemical materials. This activity will be carried out by mechanical devices that will be activated only in emergency situations. The will be installed in such a way as to allow normal manual opening and shutting of windows and doors in routine situations.
5. Automatic dispersion of masks that can help occupants of the building protect their lungs from chemical materials. This is an adaptation of a similar measure used in civilian aircraft where oxygen masks are stored in overhead cabinets that automatically open when there is a sudden drop in pressure inside the plane.
6. Automatic alerts to security and medical forces that will rush to the scene to help occupants cope with the crisis. This is an adaptation of a similar measure used to alert police or security companies in case of burglary.
7. Automatic signal system that will direct occupants safely out of the building. This measure is an adaptation of a similar technique used to lead passengers out of an aircraft in case of emergency.

5.4. Insider/ Intruders protection

The RIBS consortium engaged in the identification and dissemination of numerous vulnerabilities that relate to smart cards used in buildings worldwide. Our key results were presented at IWCC 2013, International Workshop on Cyber Crime in San Francisco in May 2013 and also in a presentation given at a French industry conference Chip to Cloud security in September 2012. During this process we have demonstrated a number of concrete exploitable vulnerabilities of access smart cards used in buildings, banks, public transportation, airports, large corporations, educational and military institutions.
We believe that our results have accelerated many upgrades in all these systems, for example the Transport for London smart card chip was upgraded as a result of this.

We have also examined new ways to improve the robustness of persistent authentication through integration of continuous multimodal remote biometrics, which was presented at the 6th SETOP Workshop at the European Symposium On Research In Computer Security (ESORICS) in London 2013. The accuracy of the multimodal remote biometrics, based on different sensors in a smart environment, has been improved through the definition of an error-rate-based fusion model that was presented at the 11th Annual Conference on Privacy, Security and Trust (PST'13) in Taragona in 2013. The remote multimodal biometrics techniques and the error-rate-based sensor fusion model have many applications in situational awareness and the use of remote biometrics in building security.

5.5. Spatial analysis

1. Development of interactive tools for spatial analysis of generic architectural interest as well as specific security interest
2. Development of the concept of spatial resilience
3. Development of specific measures of spatial resilience
4. Development of composite analysis of spatial resilience: identifying different aspects of spatial resilience, identifying measures that can respond to these aspects, and developing new measures where measures are lacking.
5. Development of increased precision in use pattern prediction in architectural solutions
6. Development of interactive and automated modeling tools
7. Development of principal modeling methods of generic architectural importance
8. Development of *generic use scripts* to integrate evaluation of impact on daily operations into security measures
9. Development of representations and models of building use/occupancy behaviour linked to architectural solutions
10. Development of infrastructure security strategies
11. Development of requirements and measurements to enable usability and integrity evaluation pre/post security measurement implementation

5.6. RIBS simulation tool

1. Development of a simulation tool with the following capability:
    - Manual crime script creation, visualisation and storage
    - Displaying the offender's view: at any point along the crime script, to allow the user to understand what the offender would see at a given point, and thus how his progression forward may be influenced
    - Event tree simulation: calculates the possible paths to an intended triggering destination, determining the probability of completing each path
    - Complex event tree simulation: calculate the possible paths to an intended triggering destination, and considers that the offender may change their mind, and trigger the weapon at any point along a given route, determining the probability of completing each path
    - Calculating the results of a biological attack at any position in the building, based on the state of the ecosystem (including status of the doors and windows, i.e. open/closed, type of weapon used, quantity of weapon used). N.B. to do this it relies on three external executables. It also displays the consequences of an attack in terms of fatalities and injuries
    - Displaying the results of an explosive attack, in terms of peak over pressure, and consequences in terms of fatalities and injuries
    - Displaying the results of a chemical attack, in terms of concentration of agent over time, and consequences in terms of fatalities and injuries
    - Displaying the nodal network of the building

- Displaying the effect of the inclusion of potential protection measures on the risk of an attack occurring (determined as a function of probability and consequences)

2. Development of a systematic method for developing graphs of building environments based on state transitions, zones and paths.
3. Development of a novel method for dynamically generating Discrete Event Tree (DET) to represent terrorist attacks.
4. Development of the first quality assurance concept for crime scripting.

5.7. Ethics

1. Development of a code of ethics for the conduct of security related projects.
2. Development of the concept of computational ethics assessment

The following lists the requirements developed using the RIBS method. The full versions of the requirements (including measurements) are available in the final deliverable.

6. PROTECTION AGAINST BIOLOGICAL THREATS (1)

L.C. Campos[*], Z. Nasar[*], M. Carpentieri[*] and L. Ciric[*]
UCL Department of Civil, Environmental and Geomatic Engineering

7. PROTECTION AGAINST BIOLOGICAL THREATS (2)

L. Ciric[*], M. Carpentieri[*], Z. Nasar[*] and L.C. Campos[*]
[+]UCL Department of Civil, Environmental and Geomatic Engineering

8. K. PROTECTION AGAINST BIOLOGICAL THREATS (4)

L. Ciric[*], M. Carpentieri[*], Z. Nasar[*] and L.C. Campos[*]
[*]UCL Department of Civil, Environmental and Geomatic Engineering

9. L. PROTECTION AGAINST CHEMICAL THREATS (1)

B. Golany[*], A. Marmur[*], T. Le Sage[+] and H. Borrion[+]
[*]Technion, [+]UCL Department of Security and Crime Science

10. PROTECTION AGAINST CHEMICAL THREATS (2)

B. Golany[*], A. Marmur[*], T. Le Sage[+], and H. Borrion[+]

[*]Technion, [+]UCL Department of Security and Crime Science

11. PROTECTION AGAINST EXPLOSIVE THREATS (1)

I. D. Petropouleas[*], N. Pappa[*] and A Karyda[*]

[*]2E

12. PROTECTION AGAINST EXPLOSIVE THREATS (2)

I. D. Petropouleas[*], N. Pappa[*] and A Karyda[*]

[*]2E

13. PROTECTION AGAINST INDIVIDUALS

M. Ingwar[*] and C. Jensen[*]

[*]DTU Department of Informatics and Mathematical Modeling

14. INFRASTRUCTURE SECURITY

D. Koch[*], C. Derix[+], P. Miranda[*], Å. Izaki[+], A. Deleuran[+], P. Jagganath[+] and H. Markhede[*]

[*]KTH School of Architecture, [+]AEDAS R&D

D. IMPACT

15. INTRODUCTION

The RIBS project has delivered protection measurements, design requirements, and a set of associated methodologies transferable to various types of infrastructures. It is expected that the project will provide a rational, credible and consistent basis for developing the next generation of physical security systems for the protection of buildings throughout Europe. The impact of RIBS will be enhanced security of buildings and infrastructures, and a reduction in the disruption of business traditionally caused by current security systems and practices. This summary sets out the various activities that have been pursued by the RIBS project to enable impact by the project's outputs.

The RIBS project aimed to impact upon a number of key audiences. These include:

- Scientific researchers working in the areas of security systems design, security systems methodologies
- Security and crime reduction practitioners working in industry, both large and SME
- Security and crime reduction practitioners working in the public sector
- Manufacturers of security equipment
- Designers of security systems
- Procurers of security systems
- Masters level and research students working in the areas of security systems design, security systems methodologies, counter terrorism

15.1. The Plan for Dissemination

When the RIBS consortium originally came together to prepare the project proposal it was unanimously agreed and understood that dissemination would be of critical importance to the project's success, and that the engagement with end-users would form a central aspect of this dissemination process. We were fortunate to have as part of the project consortium several end-users, including NBG– who were prepared to help us understand the retail sector. This early involvement with an end user as part of the core team helped us to consider in detail the requirements for a comprehensive, effective and long-lasting dissemination strategy.

The dissemination agenda for RIBS commenced after the endorsement of a dissemination strategy, agreed between the project partners. The dissemination strategy sought to empower a broad community of stakeholders and experts to partake in the exploitation and dissemination activities. The dissemination of knowledge and spreading excellence and the exploitation of the efforts and outcomes of this project commenced early in the project, from year 1, in line with our ambitious vision.

15.2. The RIBS Dissemination Strategy

The RIBS Dissemination Strategy was formally agreed as part of Deliverable 9.1. The strategy was articulated as follows:

"By involving stakeholders in the development of the project from the beginning and through a range of activities (workshops, user-groups, advisory committee, etc), the RIBS-project will directly impact on professional practices within industry (security consultants, security product designers, manufacturers, integrators), private end-users (building-owners, and security services companies) and public end-users (law enforcement agencies, government departments, etc).

The Dissemination Strategy of RIBS will aim to facilitate these planned impacts through a range of activities such as website dissemination, dissemination at specialist conferences and workshops and the creation of user groups. These activities are listed in the Dissemination Action Plan."

15.3. The RIBS Dissemination Action Plan

The Dissemination Action Plan is a list of planned activities that was set down as a roadmap to enable the Dissemination Strategy of the RIBS-project. This list is presented for ease of reference in Table 1 below, together with a column that describes how the planned dissemination was implemented, and how effective such activities have been till date and our plans for the future

Table 1: Dissemination Action Plan – List of Activities

Dissemination action	Plan	Delivery and Impact
Press releases	Press releases by RIBS partners	Various press releases and newsletters have been undertaken by the RIBS team, including a regular RIBS newsletter to a security and crime mailing list of 9000+ individuals.
Website	The RIBS Project will maintain its own website	The RIBS website was set up early in the project and has provided a key platform for dissemination activity about the project: http://www.ribs-project.eu/ To preserve the legacy and availability of the content from this website it is in the process of being migrated to a long-term servers at UCL, the project coordinator. RIBS partners have also created a web presence for RIBS on partner websites.

RIBS mailing list	Interested parties will be actively encouraged to register into a central RIBS mailing list in order to create user communities.	A mailing form was created on the project website and used to create a RIBS community of interested individuals, thus widening the dissemination of the project's outputs. We intend to keep the mailing list registration form open so that those who wish to can become involved with the post-project activity and be kept abreast of developments.
RIBS video	30 second video that describes the objectives of the RIBS project and aims to help develop our user communities.	The RIBS video was completed and may be viewed here: http://www.youtube.com/watch?v=DKdET7nfl68&feature=youtu.be The video was available on partner websites and other forums. It has been shown at a variety of RIBS events and forums and has generated excellent feedback as a means of introducing the RIBS project in an engaging way. The video will continue to be available on various websites and online forums such as YouTube.
RIBS leaflet	A short leaflet will describe the objectives of the RIBS project and aims to help develop our user communities.	The RIBS leaflet was produced twice, with a second upgraded version in the second period. Over four hundred copies have been distributed to practitioner and scientific audiences at a wide variety of RIBS events such as the RIBS workshops.
External Advisory Board	Convening of a high-level external advisory board of up to 6 individuals. This will be a senior group that provides strategic guidance & feedback at a higher level, and opens doors for project dissemination.	The RIBS Advisory Board met in year two and year three and consisted of senior individuals from the practitioner industries such as senior security chiefs from the SISTERS Banks group. For instance in 2012 the event was organised at Merrill Lynch's London Office. Sister Banks is an end-user association chaired by the Head of Security of the Bank of England designed to facilitate knowledge transfer as well as the sharing of best practices between security practitioners working in Europe's largest financial institutions. The Advisory Board provided valuable feedback and took on board results from the project to disseminate within their respective sectors.
High –level focus group	A focus group will be conducted with up to 20 key public policy stakeholders from across the EU with the ability to influence security systems development and implementation methodologies in key European industry.	This focus group took place on 21st October 2013 and involved a group of senior individuals from a broad range of public sector organisations including UK Health Protection Agency; Danish Financial Supervisory Authority.; Greek Centre for Security Studies, KEMEA; Global Resilience, Security and Risk, ARUP; Security and Resilience Network, London First; DBI - Danish Institute of Fire and Security Technology; Public Health England. The group engaged with the RIBS team to discuss project outputs and how they could be best disseminated within their own organisations and to a wider audience. Feedback from the focus group provided excellent input for the RIBS team. The group gave a strong commitment to participate in post-project activities and follow-up proposals and to help disseminate the RIBS Handbook.

Workshops	Project outcomes will be presented at a series of 4 workshops in different cities	Four major workshops were delivered: **International Crime Science Conference 2012 – *Resilient Infrastructure and Building Security*** 4th July 2012, British Library, London **Architectural Morphology:** **investigative modelling and spatial analysis** 14th May 2013, KTH School of Architecture, Stockholm **Challenges in assessing public buildings'** **resilience to bio attacks** 20th May 2013, UCL, London **Resilient Infrastructure and Building Security (FP7-RIBS)** 17th September 2013, Athens These workshops brought together a large, diverse audience of researchers, practitioners, developers, manufacturers, SMEs and public sector policy makers all interested in the outputs from the RIBS project. The events enabled a strong dissemination effort covering all aspects of the project. Aside from these four workshops a number of additional workshops were convened by RIBS partners. Our aim was to bring in 'influencers' who are involved with building planning and the implementation of security measures in those regions, and we succeeded in this objective.
End User Group	The End-user Group was intended to help with the validation and dissemination aspects of the project.	This group was created from security practitioners in the private sector including banks/financial institution managers, security professionals responsible for these types of buildings and also design companies for such systems/buildings and also users on the floor such as security officers, insurance companies. The end-user group has been involved in many aspects of RIBS, such as focus groups and workshops helping with validation and dissemination. The group will continue to be available to the RIBS team as we pursue follow-up projects (such as from the new Horizon 20-20 programme) and activities. .
Technical User Group	The Technical Group was intended to help with scientific validation of the project.	This group was created from academics and scientists from security organisations such as the UK Home Office Scientific Development Branch and the UK Centre for the Protection of National Infrastructure. The group will continue to be available to the RIBS team as we pursue follow-up projects (such as from the new Horizon 20-20 programme) and activities.
Incorporation into postgraduate taught courses / CPD training	The results of the project will be incorporated within at least one module on the Msc in Countering	The RIBS methodology was adopted as the structure underpinning the module Risk and Contingency Planning at University College London. This postgraduate module is taught to postgraduate students from a range of Master's programme, including:

	Organised Crime and Terrorism run by UCL SCS. An attempt will be made to incorporate into other taught modules or CPD courses run by the partner organisations	• MRes Security Science • MSc Countering Organised Crime and Terrorism • MSc Risk, Disaster and Resilience RIBS material has also been embedded in other courses (such as the Masters in Urban Planning & Design) by RIBS partners. Many of the students taking these courses embark in a career in the field of security in industry, public sector or academia, thus giving the RIBS project genuine long-term impact
Research publications & papers	Research papers will be published in academic and non-academic publications.	A wide variety of peer-reviewed papers and practitioner publications have emerged from the RIBS project covering the various domains of the project. This breadth of published work has helped to broaden the reach and impact of the project. Additionally a variety of practitioner-oriented publications have been published by the team, including industry briefings.
Conference presentations	Presentation by RIBS partners at conferences, workshops, symposiums and seminars of project outputs.	RIBS researchers have been exceptionally active in presenting outputs at a wide variety of forums around the world.
RIBS handbook	A user-friendly written RIBS PROJECT HANDBOOK will be created.	The RIBS HANDBOOK is under preparation and will provide a lasting impact legacy for the project. It is being prepared to be specifically of immediate benefit to practitioners from the private and public sector and will provide specific guidance derived from the project outputs that may be implemented within practitioner organisations. The Handbook is being prepared following advice from practitioners through RIBS workshops, focus groups, end-user community feedback and External Advisory Board feedback.

15.4. Summary of Dissemination Activities

A snapshot summary of the total dissemination activity for the RIBS project can be seen from Table 2 below.

Table 2

Type of dissemination activity	Number
Peer Reviewed Papers	**27**
Other Dissemination Activities as follows:	**110**
Presentations at Conferences	***41***
Workshops & Conferences	***21***
Practitioner publications	***11***
Course modules / lectures / seminars	***10***
Websites / webpages / webforums	***6***
Other activities – videos, press releases, advisory groups,	***21***

15.5. Impact Case studies

A number of case studies serve to demonstrate the clear impact of the RIBS project:

15.5.1. Impact with the Danish Institute of Fire and Security Technology

The RIBS team at DTU has held several meetings with the Danish Institute of Fire and Security Technology (DBI), where the ideas and techniques for persistent authentication, developed in the RIBS project, were presented. The DBI is Denmark's leading knowledge centre in the field of fire safety and prevention, but they also provide advice on physical security from reinforced doors and windows to the installation of strong boxes. Apart from being the national training institution for fire inspectors, the DBI offers training to security professionals who install physical security (access control systems, alarms and CCTV systems). The DBI defines national standards for fire safety and guidelines for security that are considered standards by Danish industry. Current security technologies, e.g. burglar alarms or CCTV systems, are primarily used reactively, i.e. they are used to detect a security events the moment it happens or to collect evidence that may be used to prosecute the perpetrator. The predictive powers and situational awareness offered by Persistent Authentication allows security technologies to be used pro-actively, e.g. to use CCTV cameras to recognise situations from predefined crime scripts and trigger an alarm, which allows the security system to be used as an early warning system. There is a drive in the security industry to replace human agents with technology in order to drive down costs and possibly expand the market for security technology, but the reactive application of technology in current security systems means that human agents still have a significant advantage. The

proactive use of security technology developed in the RIBS project means that technology may replace some human agents, driving down costs and expanding the domains in which security technologies will be installed. The strong interest from the DBI in the benefits offered by persistent authentication, and the continuous discussions between the RIBS team at DTU and the DBI research team, means that the results of the RIBS project will inform, and may well influence, future standards and guidelines in Danish building security. As the DBI is training many of the technicians who install security technology in Denmark, the discussions with the DBI mean that there is a genuine possibility that in the near-term future the ideas developed in the RIBS project will have an impact on practice in the Danish security industry.

15.5.2. Impact by Aedas and KTH – Influencing scientific research and postgraduate training

The research conducted by Aedas|R&D has had academic as well as professional impact: For the academic field, some of the methodologies developed by the Computational Design Research group, have influenced other university research directly, such as the medial axis (MA) representation for building structures taken up by the KTH research group. Additionally, the spatial structure methodology representation through MA will be part of a PhD at the Royal School of Arts Copenhagen. The circulation structure and visibility methodologies disseminated during a RIBS lecture and workshop at ETH Zurich have led to a common scientific validation project that is currently under development and to be started during the summer semester 2014. The academic impact of RIBS research can be further demonstrated by KTH leading the Research & Teaching Research Workshop at the 9th International Space Syntax Symposium and expanded teaching and opponent requests nationally and internationally. Through KTH, RIBS research has had direct impact in courses at Masters' and PhD level.

15.5.3. Impact by Aedas and KTH – Influencing professional practise in the built environment

Professionally, the 4 methodologies developed by Aedas CDR are undergoing transformations and further generalizations for more applied scopes in the built environment. The spatial classification method is being broadened and generalized to include also non-thread based spatial attributes. The circulation structure methodology is being generalized for resilient circulation and therefore represents direct application of RIBS development in practice. Research and development conducted on the visual risk methodology provided vital foundations for more robust professional services on visibility analysis. Observation methods developed at KTH based on methods originally established at UCL Bartlett have further spread to projects of AEDAS R&D and at DTU. Methods to analyse workplace environments have had direct impact on a parallel research project on hospital environments, through which RIBS knowledge directly reached the leaderships of Locum and Västfastigheter, two of the largest facility providers for Hospitals in Sweden, as well as staff at Karolinska Universitetssjukhuset. RIBS further has part in the initiation of cooperation with Nyréns, one of Sweden's largest architectural offices, with the aim to conduct a research by design project into future of laboratory

environments, and with GeorgiaTECH and UCL the Bartlett for future research. Furthermore, RIBS research has had continuous indirect input into the work at Patchwork Architecture Laboratory. The firm integrates research knowledge into architectural design, and also develops how often theoretically heavy and time-consuming research methodology can be translated into simpler conceptual ways of thinking and discussing architecture, and communicating design intents, solutions and possibilities with clients.

15.5.4. Impact by Aedas and KTH on organisations from the financial sector

The infrastructure domain has helped several organisations describe the way they use buildings as spatial practice; that is, how organizational distribution, routines and practices come together and distributes personnel and visitors in the object over time. It has also made concrete how visitors behave and how they move in the object. This includes making tangible some habits and patterns that were unknown, and clarifying some that were tacitly known but difficult to point to. Specifically, the infrastructure work has further provided a greater understanding about how the above elements relate to the spatial structure of the buildings considered. Furthermore, it has added understanding of how spatial properties of visibility and permeability impact operations, public relations and security.

15.5.5. Impact by 2E - Security Consulting Company formation

Inspired by the RIBS project and interaction with RIBS consortium members Iakovos Petropouleas of 2E formed “Otrym Consulting”. Otrym Consulting is a provider of integrated active risk mitigation and control solutions for corporations as well as private individuals. It offers uncompromising on-the-ground crisis management and response. Otrym helps manage crises and protect clients interests both home and abroad. It does so through adapting experiences gained thorough interaction with RIBS partners and activities to clients’ corporate and personal security needs. People and situations may change, but Otrym’s operational philosophy offers an integrated approach to problem solving that was developed by interacting with RIBS members. By leveraging the diverse knowledge gained through RIBS, Otrym is able to protect clients and their assets. Otrym Consulting operates in Greece under VAT registration number: 800456369. Its website is www.otrym.com

15.5.6. Impact by 2E - Insurance Company Engagement

Throughout RIBS project various meeting were held with two major insurance companies (Interamerican, Greece and UIB, UK). Throughout these meetings the rationale behind protecting assets from terrorist threats where discussed and the importance of protecting buildings against terrorist threats where highlighted. Buildings are insured for various kinds of threats and by 2E highlighting the existing as well as possible future developments helped rationalise and quantify the effect this would have to the protection of a building in terms of reducing insurance premiums and calculating the modified insurable risks, before as well as after the implementations of suggested security measures.

15.5.7. Impact by 2E - Law Firm Engagement

Throughout RIBS project various meeting were held with two major law companies (Laskos Law, Greece and DLA Piper, UK). Both law firms demonstrated a great interest in the levels of protection that can be achieved from implementing additional security measures in building already in operation. This will assist them in understudying the associated risk from a legal standpoint and will able them to effectively define the implications of protecting ones assets in terms of legal liability (both civil as well as criminal) in the case of an attack from the standpoint of a building owner and/or operator

15.5.8. Impact by 2E - SimTec Hellas

SimTec is the Greek representative of ANSYS. When 2E first approached SimTec in order to purchase the ANSYS suite software used to conduct the explosion modelling required from RIBS, SimTec staff was not aware of the software capabilities and the fine details of explosive engineering. Throughout their interaction with RIBS researchers both sides gained considerable amounts of knowledge on modelling explosions using software tools. The input from RIBS project was deemed so unique and important that SimTec chose to show case it on their 10 Year anniversary edition book.

15.5.9. Impact by 2E -SIKA Hellas

SIKA is an international provider of FRP materials for building reinforcement. While they are very knowledgeable on the capabilities of their products for earthquake strengthening they were not aware of the possibility that their products could be used of blast protection. They provided information on the performance of FRPs that was used in RIBS simulations and in turned were briefed in possible uses of their products in protecting buildings against blast.

15.5.10. Impact by 2E - SKYDAS Lithuania

Skydas is a manufacturer of armoured doors and windows based in Lithuania that produce as well as distribute their products throughout the world. They provided information on vendable doors and windows that were used in case of internal gas and dust explosions. In turned they were advised on the requirements for possibly modify their products to accommodate venting in the case of high explosive detonations.

15.5.11. Impact by UCL – Training the next generation of security professionals

The RIBS methodology was adopted as the structure underpinning the module 'Risk and Contingency Planning' at University College London. A group project approach is used to encourage students to learn and apply security risk theories. This postgraduate module is taught to over 30 postgraduate students from a range of Master's programme, including:

- MRes Security Science (Preparation year for the PhD in Security Science)
- MSc Countering Organised Crime and Terrorism
- MSc Risk, Disaster and Resilience

Several of the students taking these courses later embark in a career in the field of security in industry, public sector or academia, which guarantees another form of dissemination of the RIBS methodology in future.

15.5.12. Impact statement from a representative organisation from the financial sector

"The RIBS research project team worked closely with various stakeholders within our organization (Executive Management, Physical Security Division, Technical Projects Division and Internal Audit). The team applied a well structured approach to collect and analyze real life environment data from one of our Headquarter Buildings, in an effort to produce specification of requirements that would be used to produce effective and affordable protection measures. Our organization reaped several benefits from its participation to the RIBS project. Firstly, it was exposed to a number of new innovative analysis techniques such as "spatial analysis", "crime scripts simulation" and others. Secondly, it had the opportunity to identify potential weaknesses to our building's security measures during the analysis process and to take corrective actions where possible. Thirdly, it was exposed to a new scientific approach in assessing threats and exploitable points that could supplement our existing risk assessment approach. Finally, we had the benefit to study the project deliverables and to get exposed to a new philosophy of dealing with potential terrorist threats that would help our counter-terrorism strategy in the future. We view the RIBS project as a glimpse to tomorrow's policies and technologies that will be designed to assist stakeholders to deter and detect attack plans by terrorist organizations."

15.6. Conclusion

The RIBS project began with a promise of providing "a rational, credible and consistent basis for developing the next generation of physical security systems for the protection of buildings throughout Europe." The project has delivered on this promise by delivering protection measurements, design requirements, and a set of associated methodologies transferable to various types of infrastructures. The extensive dissemination activity from the project has served to promote these outputs through a wide variety of audiences resulting in genuine, long term impact.

E. Website and contact details

Information about the RIBS project will be available at **http://www.ucl.ac.uk/jdi**

AEDAS ARCHITECTS LIMITED

Contact: Christian.Derix@aedas.com

Infrastructure analysis team

Christian Derix, Ralfos Bakolas Pablo Miranda Carranza, Dr Lucy Helme, Prarthana Jagannath, Åsmund Izaki (formerly Gamlesaeter), Anders Holden Deleuran.

DANMARKS TEKNISKE UNIVERSITET

Contact: cdj@imm.dtu.dk

Intruder and Insider protection team

Dr Christian Jensen (team leader), Mads Ingmar

H.PETROPOULEA&CO (2E)

Contact: i.petropouleas@2-epsilon.gr

Explosive security team

Iakovos D. Petropouleas (team leader), Natalia Pappa and Agy Karyda

KUNGLIGA TEKNISKA HOEGSKOLAN

Contact: daniel.koch@arch.kth.se

Spatial analysis team

Dr Daniel Koch (team leader), Pablo Miranda Carranza, t. lic. Henrik Markhede

---

TECHNION - ISRAEL INSTITUTE OF TECHNOLOGY

Contact: marmur@technion.ac.il

Chemical security team

Prof Avi Marmur (team leader), Prof Boaz Golany, Ben Levav, and Aviah, Yaloz.

UNIVERSITY COLLEGE LONDON

Contact: Dr Hervé Borrion, h.borrion@ucl.ac.uk

Project Coordination and Dissemination:

Dr Hervé Borrion (Principal Investigator), Beth Jackson, Vaseem Khan

Attack modelling team

Dr Hervé Borrion (team leader), Dr Noémie Bouhana, Dr Tanya Le Sage, Dr Sonia Toubaline, Stavros Ioannis Tsompanidis.

Bio security team

Period 1: Dr Kaman Lai (team leader), Dr Jonathon Taylor,

Period 2: Dr Luiza Campos (team leader), Dr Matteo Carpentieri, Dr Lena Ciric, Dr Zaheer Nasar.

Intruder and Insider protection team

Dr Nicolas Courtois, Dr Daniel Hulme

Ethics and legal expert

Mr Timothy Mitchener-Nissen

NATIONAL BANK OF GREECE S.A.

Contact: kaloritis.georgios@nbg.gr

Business domain team

Georgios Kaloritis (team leader), Amalia Kalogridi, Hrysa Veletza