



CitySCAPE Italian Web Conference 2021

Advanced approach to economic impact and cost-benefit analysis

Pietro De Vito, Project Manager in CitySCAPE
STAM S.r.l.

15 December 2021

Who are we?

STAM is an engineering company that supports its clients in addressing new business opportunities and technological challenges by leveraging multidisciplinary expertise and practical experience in four major industrial sectors.



Security & Logistics



Space & Defence



Energy, circular and sustainable economy



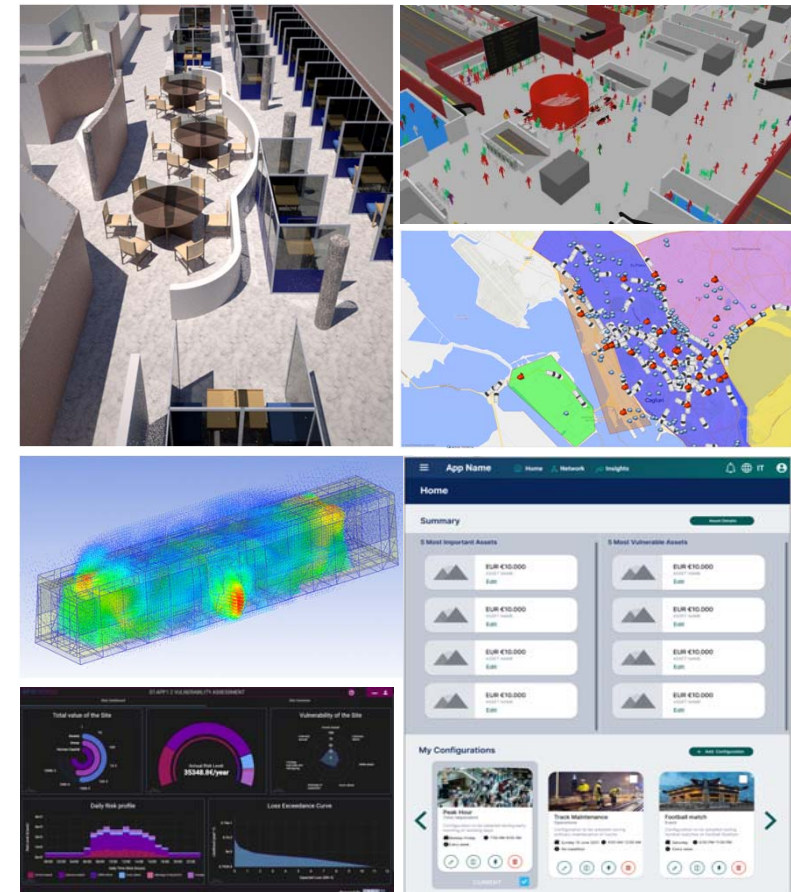
Industry & Automation



Modelling & Simulation Area



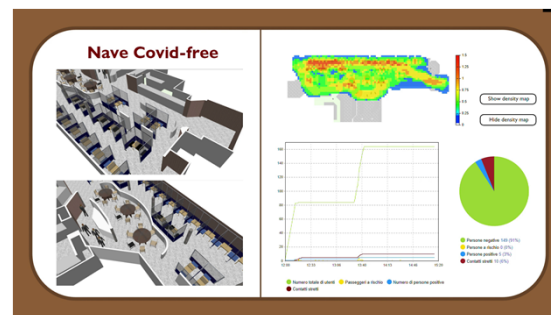
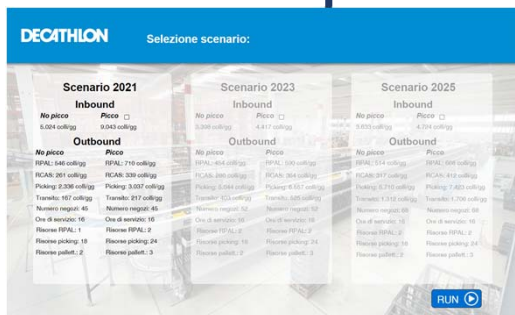
- **Modelling and simulation** of complex systems and processes
- **Assessment of the security risk** of critical infrastructures and soft targets
- **Cost benefit** analysis
- **Modelling & Simulation** of the crowd
- **Optimization and Simulation** of flows (logistics, traffic, processes, etc.)
- **Simulation of different scenarios** (e.g., terrorist attacks, pandemic, crisis, etc.)
- **Virtual assessment** of solutions and procedures



Key Assets of M&S Area

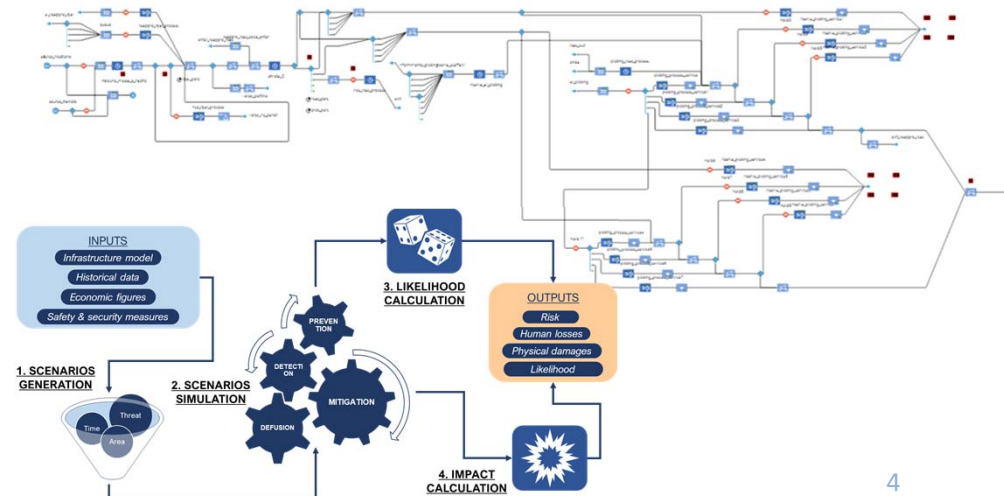
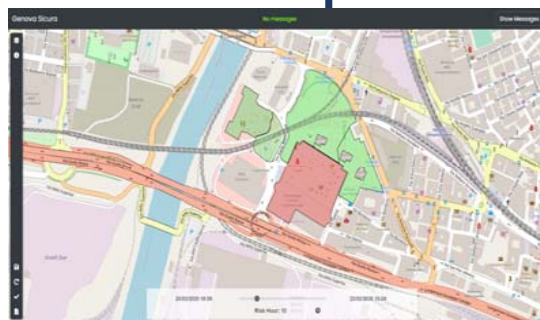
Stand-alone Simulators

Software Licenses



M&S Methodologies

Decision Support Tool



Cost Benefit Analysis



What is a Cost-Benefit Analysis (CBA)?

○CBA is a mathematical tool used in decision making to determine whether the perceived benefits exceed the projected costs of a project, providing information and estimates on the project's return on investment.

○Cost is the value of money that has been used to produce something, and is therefore no longer available.

○Benefits are the monetary values of the desirable consequences of economic policies and decisions.

○Non-recurring costs: Costs for the project defined as one-off.

○Recurring costs: Costs that are incurred periodically or for a specified period of time.

○Quantitative benefits: reduction of dedicated administrative staff and storage space.

○Qualitative benefits: improved response times and decision making.

Cost Benefit Analysis pillars



○There has to be a common unit of measure.

○The benefits are usually measured by market choices.

○Mainly based on Net Present Value (NPV):

- It is the difference between the present value of a benefit and the present value of the cost after the rate of return has been applied to it.
- The NPV to be acceptable must be > 0

Cost

Benefit

Analysis



Our approach

- The STAM approach for cost-benefit analysis is based on the results obtained from the risk assessments generated by Risk Assessment tools.
- Among the parameters taken into account in the analysis, the following are taken into account:
 - ✓ The economic value of the tangible asset.
 - ✓ The prolificacy of the services provided by the organization, and the percentage of revenues associated with each customization service.
 - ✓ The integrity of an asset, which provides an indication of the cost required for a particular asset intervention
 - ✓ The integrity of the service, which helps to estimate the downtime and the related economic losses.

Our approach

- Subsequently, it is essential to consider the evaluation of the investment required for a new security measure. The latter is characterized by two economic indicators:
 - CAPEX, which includes the cost of acquiring a new (one-off) security measure.
 - OPEX, which includes the costs for maintenance and maintenance of the security measure. (Includes annual / monthly costs of licenses, or personnel involved in maintenance)
- It is also important to consider that costs can be of two types:
 - Proactive: for example related to information gathering and debugging the installation, as well as maintenance costs
 - Responsive: associated with a faster and more effective response to be applied in order not to incur an increase in downtime along with the resources needed to repair systems.

Our approach



Intangible assets:
such as the reputation and brand value of the
organization.



Tangible assets:
All those assets that can be physically damaged and
that can cause disservices



FIMCA

Financial IMpaCt Assessment engine

Our approach



The main economic indicator that will be considered is the Return on Sustainability Investment, that is the ROSI:

$$ROSI = \frac{ALE - mALE - \text{Cost of the solution}}{\text{Cost of the solution}}$$

- Where ALE is the annual monetary loss associated with a specific risk.
- While mALE is the modified parameter to implement the security measure.

ROSI evaluates the return on investment, establishing in this sense how many losses have been avoided thanks to that particular investment.

CIS Controls



For the countermeasures we referred to the CIS Control (Center of Internet Security) which are 18 categories of security measures divided by activity and application target. Each of them contains several specific security measures. In all there are 156 and refer for example to physical systems, data protection, or defence against malware attacks.

The security measures of the CIS Controls are in turn assigned to a particular implementation group:

- IG1, security measures based on minimum security standards
- IG2, more specific security measures than IG1
- IG3, includes all possible security measures





CIS Controls

Currently, there are ongoing activities to better adapt the CIS Controls to the context of CitySCAPE. In this sense, efforts are focusing on:

- Estimate the costs of implementing countermeasures (CAPEX and OPEX).
- Map the CIS Controls to the threats that will be considered in CitySCAPE.
- Business value attribution which will then be used by the Risk Assessment tool (RITA) to assess the residual risk. These business values refer to Confidentiality, Integrity and Availability (as per ISO 27001).





The 18 groups of CIS Control

CONTROL 01 Inventory and Control of Enterprise Assets 5 Safeguards IG1 2/5 IG2 4/5 IG3 5/5	CONTROL 02 Inventory and Control of Software Assets 7 Safeguards IG1 3/7 IG2 6/7 IG3 7/7	CONTROL 03 Data Protection 14 Safeguards IG1 6/14 IG2 12/14 IG3 14/14
CONTROL 04 Secure Configuration of Enterprise Assets and Software 12 Safeguards IG1 7/12 IG2 11/12 IG3 12/12	CONTROL 05 Account Management 6 Safeguards IG1 4/6 IG2 6/6 IG3 6/6	CONTROL 06 Access Control Management 8 Safeguards IG1 5/8 IG2 7/8 IG3 8/8
CONTROL 07 Continuous Vulnerability Management 7 Safeguards IG1 4/7 IG2 7/7 IG3 7/7	CONTROL 08 Audit Log Management 12 Safeguards IG1 3/12 IG2 11/12 IG3 12/12	CONTROL 09 Email and Web Browser Protections 7 Safeguards IG1 2/7 IG2 6/7 IG3 7/7
CONTROL 10 Malware Defenses 7 Safeguards IG1 3/7 IG2 7/7 IG3 7/7	CONTROL 11 Data Recovery 5 Safeguards IG1 4/5 IG2 5/5 IG3 5/5	CONTROL 12 Network Infrastructure Management 8 Safeguards IG1 1/8 IG2 7/8 IG3 8/8
CONTROL 13 Network Monitoring and Defense 11 Safeguards IG1 0/11 IG2 6/11 IG3 11/11	CONTROL 14 Security Awareness and Skills Training 9 Safeguards IG1 8/9 IG2 9/9 IG3 9/9	CONTROL 15 Service Provider Management 7 Safeguards IG1 1/7 IG2 4/7 IG3 7/7
CONTROL 16 Applications Software Security 14 Safeguards IG1 0/14 IG2 11/14 IG3 14/14	CONTROL 17 Incident Response Management 9 Safeguards IG1 3/9 IG2 8/9 IG3 9/9	CONTROL 18 Penetration Testing 5 Safeguards IG1 0/5 IG2 3/5 IG3 5/5

FIMCA Tool (ENG)



CRISIS

Define Economic Values

Asset 1

Asset Category

Asset 1

Pessimistic Value

Placeholder

Most Common value

Placeholder

Optimistic Value

Placeholder

Alfa & Beta Calculation

Sum Pessimistic Values:

16

Sum Most Common Values:

29

Sum Optimistic Values:

42

$$\alpha = \frac{4b + c - 5a}{c - a}$$

Alfa

3

$$\beta = \frac{5c - a - 4b}{c - a}$$

Beta

3

Monte Carlo Simulations

Simulations	1	2	3	4	5	n
Placeholder	29	36	19	36	30			

Descriptive Statistic

Minimum	Average Cost - ALE: average cost that refers to asset 1 + asset 2 + assetx	Maximum
19	29	36

FIMCA Tool (ENG)



ROSI ANALYSIS

ALE: average cost that refers to asset 1 + asset 2 + asset x

mALE: could assume different value for the IG1 (Implementation Group 1) is effective in mitigating 62% of all Techniques in the MITRE ATT&CK model

The CIS Controls (IG1, IG2 and IG3) are effective in mitigating 83% of all Techniques in the MITRE ATT&CK Model.

Cost of the solution: SUM of the cost of the countermeasure 1 + cost countermeasure 2 + cost countermeasure x

Risk 1

ROSI 1

ROSI 1

☐ Countermeasure 1

☒ Countermeasure 2

☒ Countermeasure 3

☐ Label

☐ Label

☐ Label

Back

ROSI

ALE: Average Cost: 7

mALE: 80%

Cost Of The Solution

15000

$$ROSI = \frac{ALE - mALE - \text{Cost of the solution}}{\text{Cost of the solution}}$$

Description	Assets	Countermeasures	ROSI
ROSI 1	14	14	%
ROSI 2	7	14	%
ROSI 3	32	14	%

Home

Network Tree

Select a Network element to add Configuration

- Baseline
 - AVM (Automated Vehicle Monitoring)
 - OS
 - Computational Device
 - OS Data
 - HW Interface
 - Application Keys
 - Web API
 - Native API
 - OS Services
 - Storage
 - Application Database
 - Network Stack Wired (TCP)
 - Network Interface Wired (Ethernet)
 - Web Service
 - Network Controller
 - Application Data
- Passenger Mobile Device and A
- Smart Display
- Subscription System
- Ticketing System
- Validator Mobile Device and A

Home

Configurazioni che stai comparando

Configurazione Iniziale

New Configuration 2

Configurazione Corrente

Baseline

Riepilogo

Ottimo lavoro!
Il valore ROSI della configurazione corrente è incrementata di +23%!

Grafico di Efficienza media

Il grafico seguente mostra e compara il livello di implementazione medio dei CIS Control per ogni configurazione selezionata.

34%

Indice Economico

Lorem ipsum dolor sit amet, consectetur adipiscing elit. In vulputate ligula vitae augue efficitur malesuada. Maecenas fringilla purus vitae laoreet consectetur.

Grafico ROSI

Report

Your organization presents **medium** weaknesses in the following CIS control groups:

- ✓ CIS1
- ✓ CIS4
- ✓ CIS7
- ✓ CIS8

Please, take into account the implementation of appropriate security measures to address these weaknesses.



Home

Save

Tot. OPEX: 23.5294 € 100 %

EX: 0 € Tot. OPEX: 300 € 0 %

Any questions?

Thank you!



Pietro De Vito

 p.devito@stamtech.com



This project has received funding from the EU's Research and Innovation programme Horizon 2020 under grant agreement No 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.