Co-funded by the
Erasmus+ Programme
of the European Union

SPECIAL MOBILITY STRAND

Physical protection systems of critical infrastructure objects and their vulnerability assessment

Tomáš Loveček

Tirana/Albania

2019-03-11

Work experience

• Dates	*2015 – present*
• Name of organisation	University of Žilina, Faculty of Security Engineering, Department of Security and Safety Research
• Occupation or position held	**Head of Department**
• Dates	*2012 – 2015*
• Name of organisation	*NATO (The Science for Peace and Security Programme)*
• Occupation or position held	**Project Evaluator**
• Dates	*2011 – 2015*
• Name of organisation	University of Žilina, Faculty of Security Engineering
• Occupation or position held	**Vice-dean for Science and Research**
• Dates	*2007 – 2011*
• Name of organisation	University of Žilina, Faculty of Special Engineering
• Occupation or position held	**Vice-dean for Development and Foreing relations**
• Dates	*2015 – present*
• Name of organisation	University of Žilina Faculty of Security Engineering – Department of Security and Safety Research
• Occupation or position held	**Full Professor**

Co-funded by the
Erasmus+ Programme
of the European Union

Text books...

Video Surveillance Systems

2007 2008 2012 2015

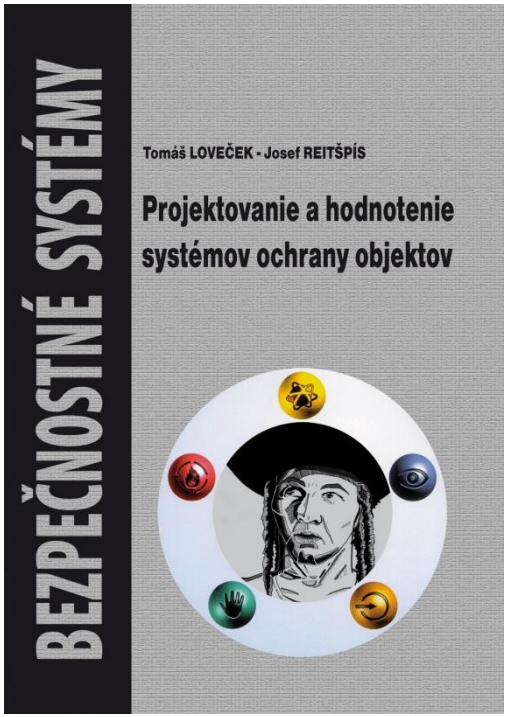
Security of Information Systems **Alarm systems**

Co-funded by the Erasmus+ Programme of the European Union

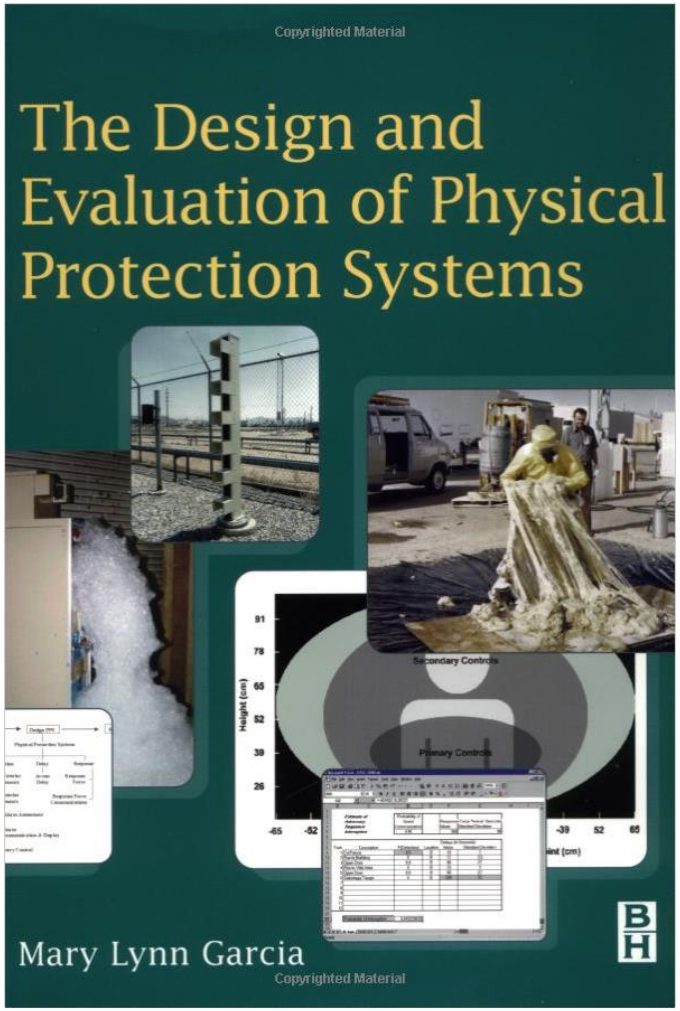
Text book & Monography...

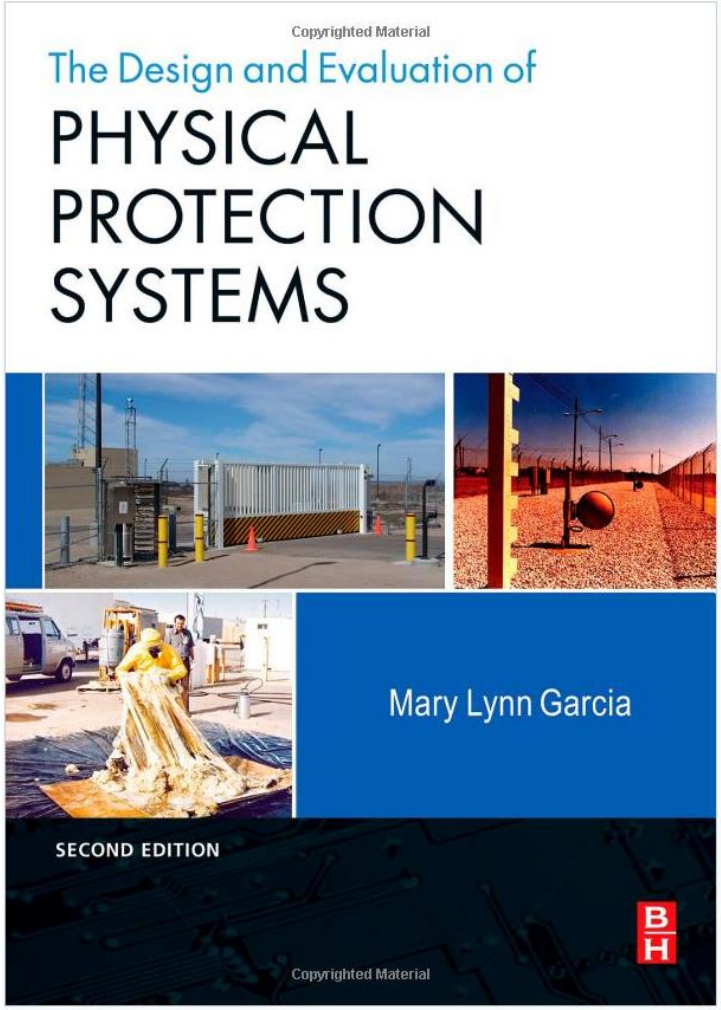
Planning and Designing of PPS/ *Tomáš Loveček, Ladislav Mariš, Anton Šiser ; 1. vyd. - Žilina : Žilinská univerzita, 2018. 285 s. ISBN 978-80-554-1482-9*

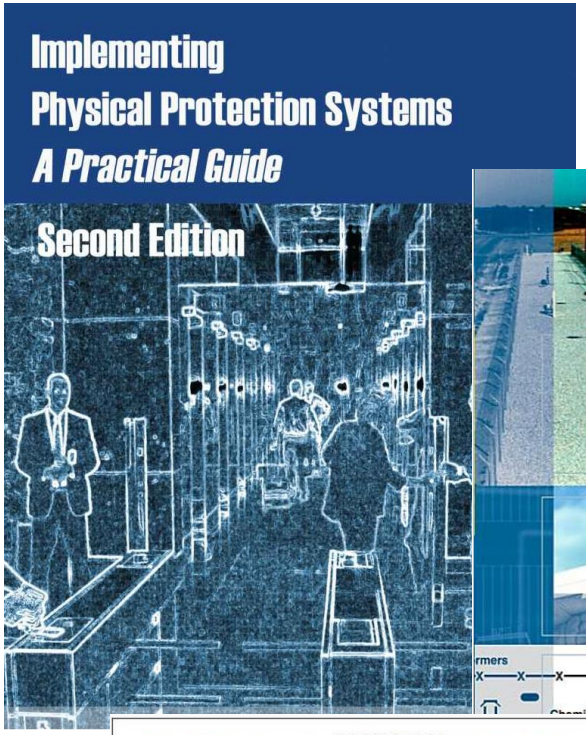
Designing and Evaluating of PPS/ *Tomáš Loveček, Josef Reitšpís ; Žilina : Žilinská univerzita, 2011. 281 s., ISBN 978-80-554-0457-8*

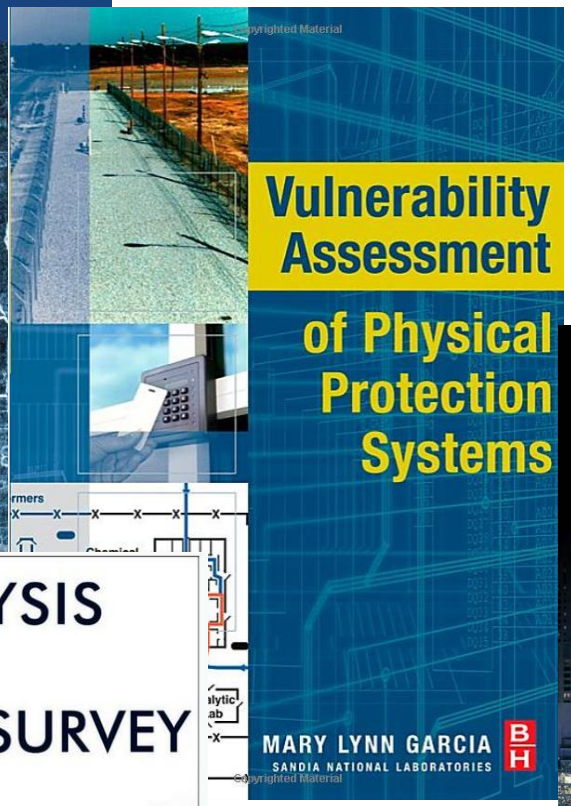


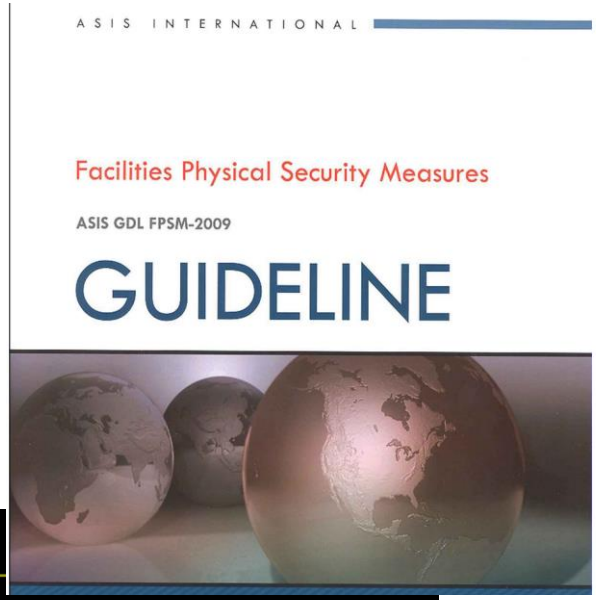
Co-funded by the Erasmus+ Programme of the European Union

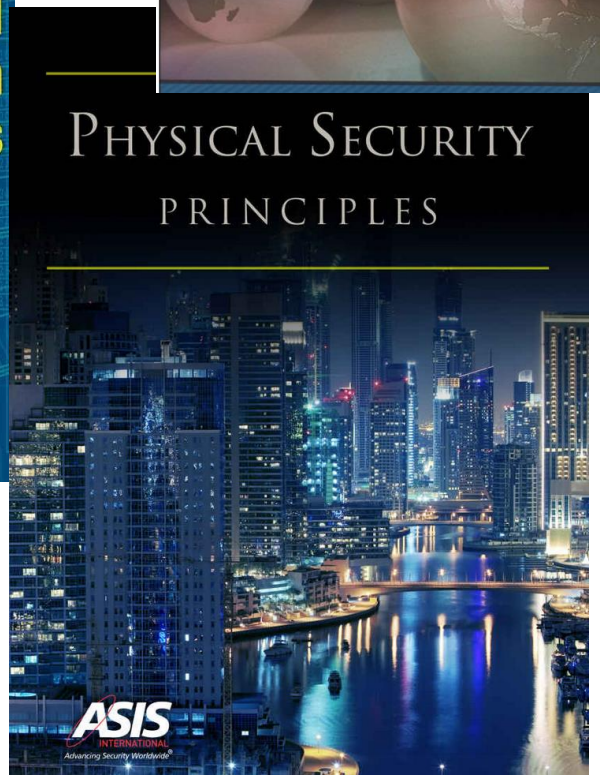

Copyrighted Material
The Design and Evaluation of Physical Protection Systems
Secondary Controls
Primary Controls
Mary Lynn Garcia
Copyrighted Material

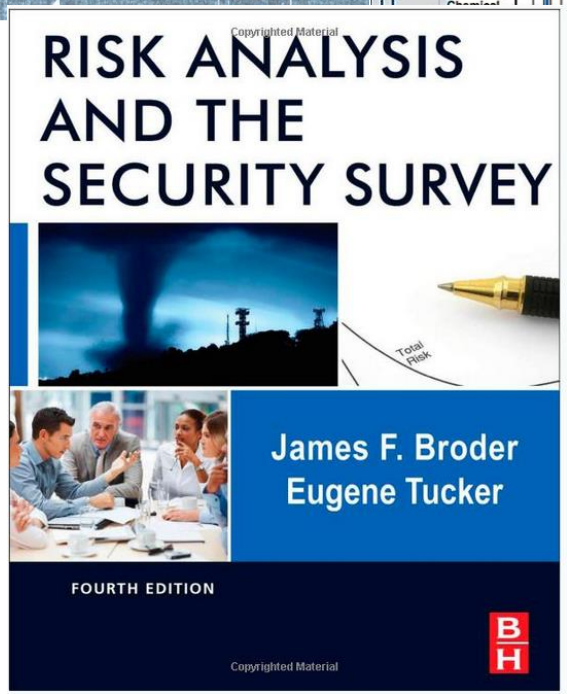

Copyrighted Material
The Design and Evaluation of
PHYSICAL PROTECTION SYSTEMS
Mary Lynn Garcia
SECOND EDITION
Copyrighted Material


Implementing
Physical Protection Systems
A Practical Guide
Second Edition


Vulnerability Assessment
of Physical Protection Systems
MARY LYNN GARCIA
SANDIA NATIONAL LABORATORIES
B H


ASIS INTERNATIONAL
Facilities Physical Security Measures
ASIS GDL FPSM-2009
GUIDELINE


PHYSICAL SECURITY
PRINCIPLES
ASIS INTERNATIONAL
Advancing Security Worldwide


RISK ANALYSIS AND THE SECURITY SURVEY
James F. Broder
Eugene Tucker
FOURTH EDITION
B H

Projects...

Critical Infrastructure Protection Against Chemical Attack – CIPAC, *2013/CIPS/AG/4000005073*

Methodology for physical protection assessment of critical infrastructure elements agaist terrorist and other types of attacks – PACITA, *HOME/2010/CIPS/AG/044*

Competency Based e-portal of Security and Safety Engineering – eSEC (www.esecportal.eu)
502092-LLP-1-2009-1-SK-ERASMUS-EMHE, 2010-261814

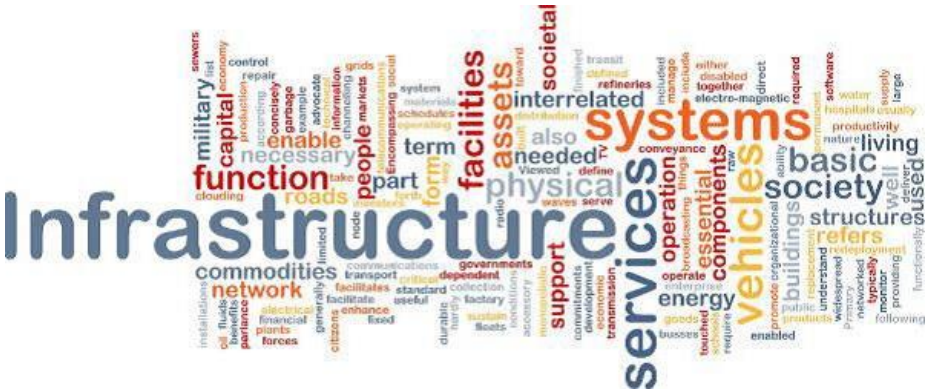
The Community Based Comprehensive Recovery – COBACORE, *2012-313308*

Co-funded by the
Erasmus+ Programme
of the European Union

Introduction

The term “infrastructure” has various meanings in technical literature and practice and various points of view of the topic are described by various authors according to their area of interest and expertise.

Linguistically, the term infrastructure originates in Latin words “infra” (i.e. “under”) and “structure” (i.e. “building, construction”).



Co-funded by the
Erasmus+ Programme
of the European Union

Introduction

In the European Union documentation, **critical infrastructure** is defined as a component, system or their part located in the member states of EU that is necessary for maintaining the basic functionality of the society, health, protection, life quality of the residents from its economic and social point of view.

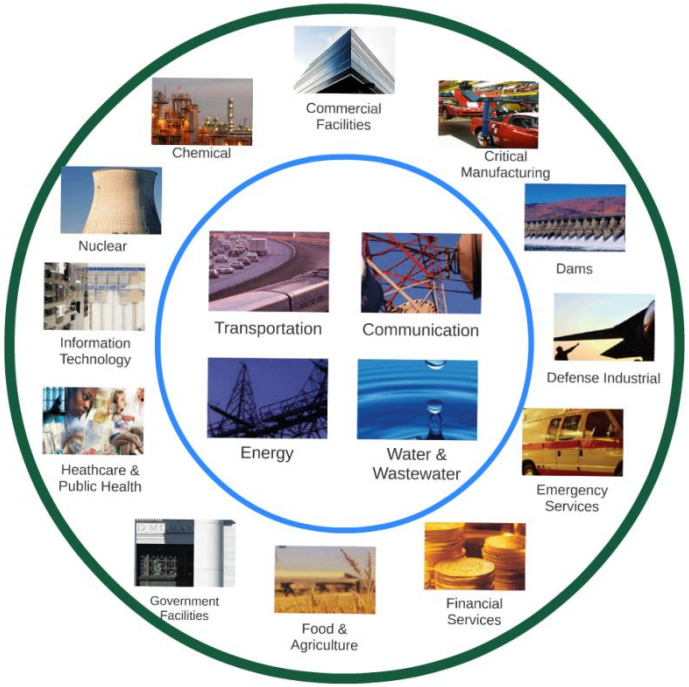
Its disruption or destruction would have serious impact on the member states due to the impossibility to maintain the functionality. (Directive 114/2008).

Co-funded by the
Erasmus+ Programme
of the European Union

Introduction

Basic critical infrastructure sectors have been outlined in the Directive, including:

transport,
energetics,
information and communication technology,
water,
food,
health,
finance,
public order and internal security,
industry.



Co-funded by the Erasmus+ Programme of the European Union

Physical protection systems of CI objects

Existing legislative regulations in the EU define requirements for physical protection measures of the critical infrastructure.

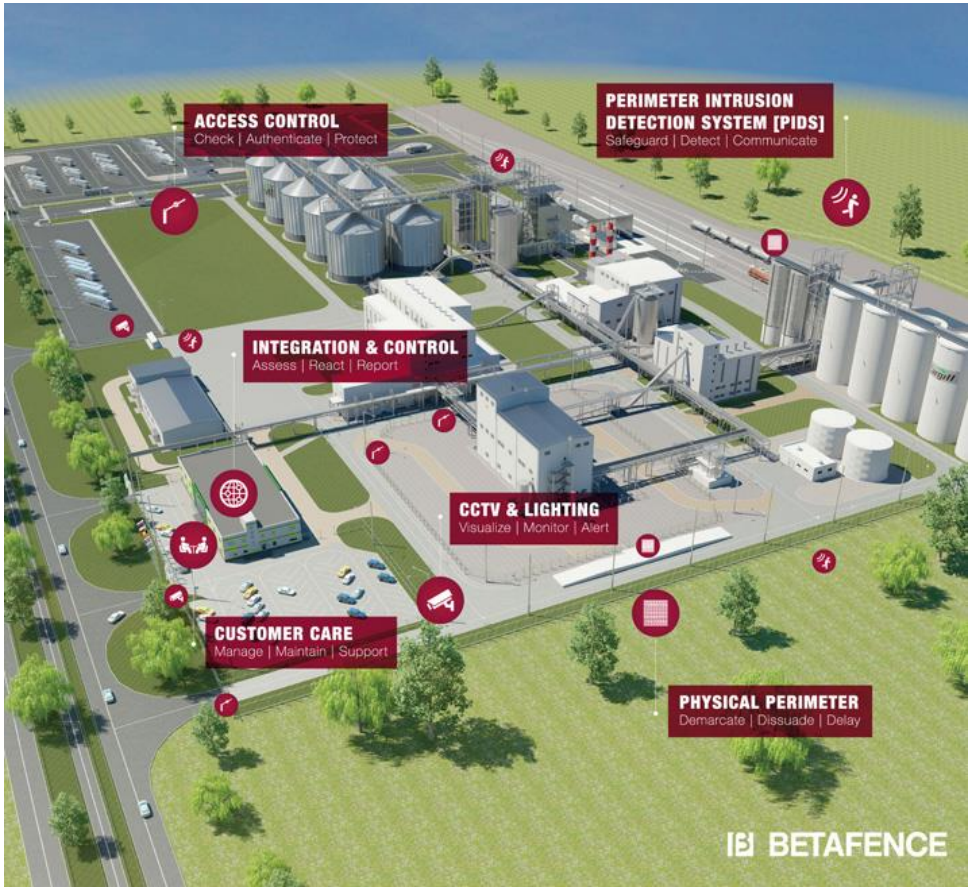
The Green paper (2005) specify possible ways (tools) to increase prevention, protection, preparedness and response within the critical infrastructure protection under the EU conditions or environments.

Co-funded by the
Erasmus+ Programme
of the European Union

Physical protection systems of CI objects

"**To reduce risk to the critical infrastructure, the technical measures** for discouraging, detection, verification, signalisation and elimination of the intruder and activity of the security services (e.g. security teams and armed forces) **can be used**."

Green Paper, 2005



Co-funded by the Erasmus+ Programme of the European Union

Physical protection systems (PPS) of CI objects

Generally, the system means a purposefully defined set of elements (their parameters and properties) and a set of relationships between them that jointly determine behaviour and functionality of the system as a whole.

System, which includes individual subsystems which has been created by purposeful arrangement/designing of protection measures, is called by various names in practice.

Two terms that describe the protection systems of property are normally used in the English speaking countries: **Physical Protection System (PPS)** and **Security System**.

Co-funded by the
Erasmus+ Programme
of the European Union

Physical protection systems of CI objects

The term **protection system** means a system realised by mechanical-technical, personal and regime protection measures or features.

Protection measures are divided into:

- passive protection measures,
- active protection measures,
- physical protection measures,
- regime-organisational measures.

Co-funded by the
Erasmus+ Programme
of the European Union

Physical protection systems of CI objects

Passive protection measures as a part of classical protection are represented by mechanical Barriers, such as:

- building constructions,
- openings (doors, windows, grades),
- secure storage units or lockers,
- security glass or foils,
- other barriers (e.g. retarders, fences).

Passive protection measures are intended for deter, retard or stop an intruder.

Co-funded by the
Erasmus+ Programme
of the European Union

Physical protection systems of CI objects

Active protection measures as a part of technical protection are represented by Alarm Systems, including:

- Intruder Alarm System,
- Surveillance Monitoring System,
- Access Control system,
- Fire Detection System.

Active protection measures are given to detect an intruder.

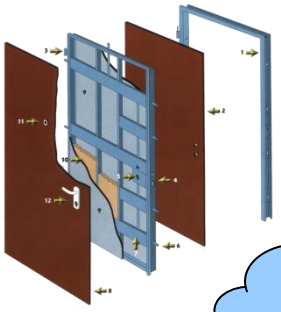
Co-funded by the
Erasmus+ Programme
of the European Union

Physical protection systems of CI objects

Physical protection measures (guarding) ensure timely intervention and elimination of the intruder and can by realize by self protection (e.g. neighbourhood watch) or profesional Security Services (state or private).

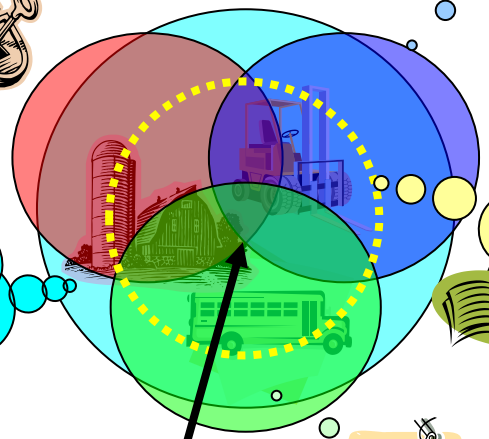
Regime protection measures ensure correct and effective operation of installed active or passive protection measures.

Co-funded by the
Erasmus+ Programme
of the European Union



Mechanical Barriers

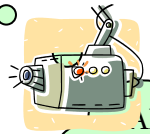
Security Services



Assets/CI

Regime measures

Minimal level protection



Alarm Systems

Co-funded by the Erasmus+ Programme of the European Union

Risk management in process of designing and evaluating of PPS

In many cases, the set up of a minimum protection level is connected to the risk management process, where the requirements for protection measures increase with an increasing of risk level (e.g. with risk level increasing the “security level “ for alarm systems).

If the risk management process does not impact on the resulting of minimal protection level, it has still a significant impact on the determination of the placement of protective measure elements (e.g. cameras, detectors, mechanical barriers, etc.)

Co-funded by the
Erasmus+ Programme
of the European Union

Risk management in process of designing and evaluating of PPS

The **approach/methodology for the risk assessment** process related to the protection of premises or buildings against intentional anthropogenic threats (f.e. organised crime, terrorists, vandalism) is given by international and national legislation and technical standards for a particular area of application, for example:

- classified information,
- **protection of critical infrastructure,**
- protection of banking subjects,
- protection of commercial and administrative premises or protection of residential premises, etc..

Co-funded by the
Erasmus+ Programme
of the European Union

ISO 31 000 Risk management

The general principles and guidance on how to approach the risk management process are defined in international standard **ISO 31 000 Risk management. Principles and instructions.**

Many of the mentioned areas of applications do not adapt with this standard, either from a terminological or a procedural point of view. Even where the relevant regulation directly refers to this standard (e.g. ISO/IEC 27005 Information technology - Security techniques - Information security risk management).

Co-funded by the
Erasmus+ Programme
of the European Union

ISO 31 000 Risk management

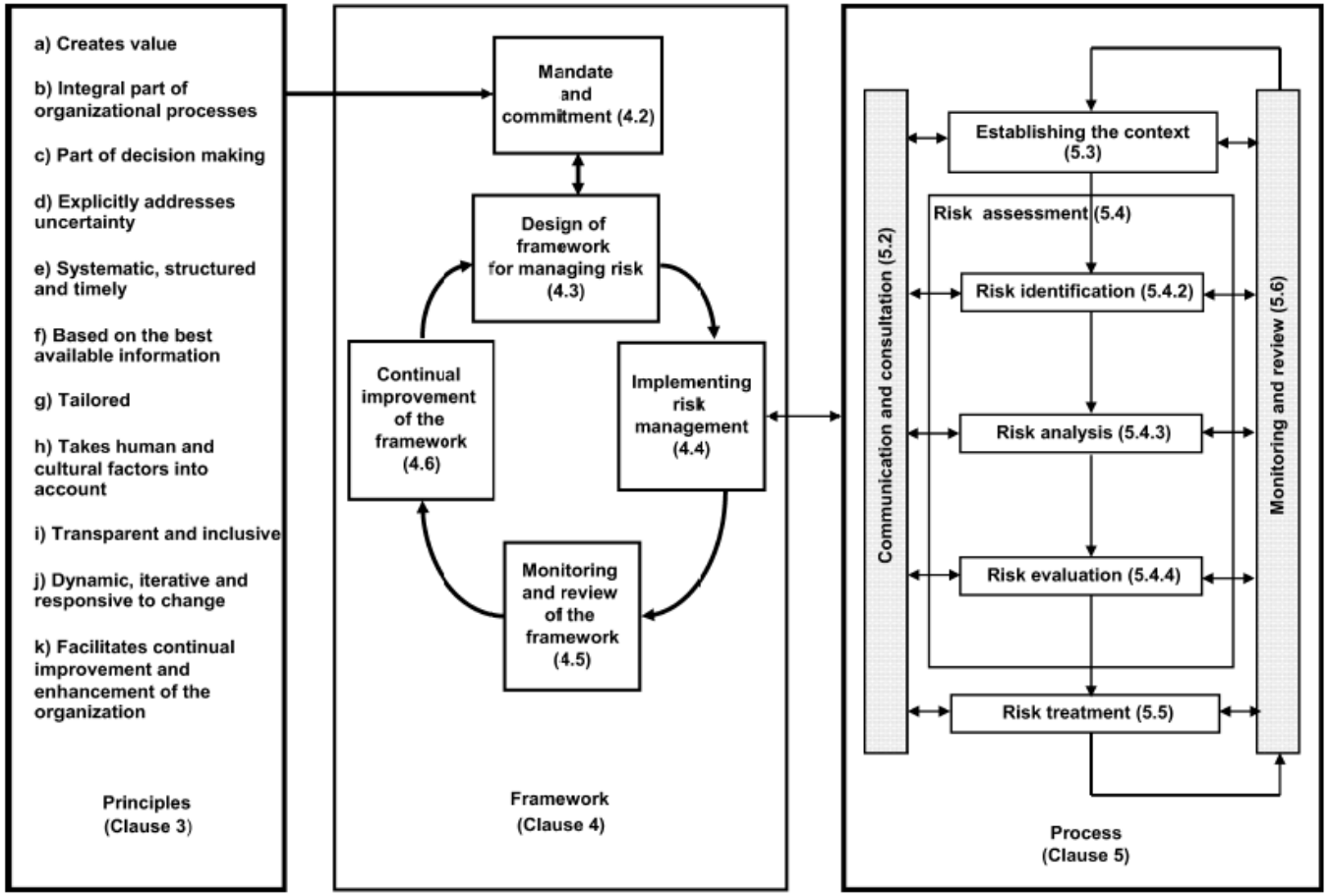
The standard can be used during the existence of any public or private organisations, associations and for individuals in a wide range of activities and processes related to decision making, operations (production, service), project preparation **and, last but not least, property protection.**

It can be applied to any type of risk of any nature, regardless if it has positive or negative consequences.

It can also be applied at different levels.

Co-funded by the
Erasmus+ Programme
of the European Union

ISO 31 000 Risk management



Co-funded by the Erasmus+ Programme of the European Union

Risk management in process of designing and evaluating of PPS

ISO 31 000 can also be applied at different levels.

An example of the use of the risk assessment process at different levels is the *Critical Infrastructure Act*, which requires from the central authority to develop sector risk analysis and update it on a given critical infrastructure segment.

At the same time, the Act obligate to the operator of a CI to assess the risk of the threat of demage or destruction of equipments (scenarios), their vulnerable sites, the consequences of disruption or destruction of the functionality, integrity and continuity of the element.

Co-funded by the
Erasmus+ Programme
of the European Union

Risk management in process of designing and evaluating of PPS

From the viewpoint of security systems designing and evaluating, the risk assessment process may be used at different levels, namely:

- the establishment of a minimum level of protection,
- **placement of systems and their protective measure elements (e.g. where placing cameras or detector in premises),**
- in the case of risk assessment related to project management.

Co-funded by the Erasmus+ Programme of the European Union

Vulnerability assessment…

If we assess risks where the consequences are constant, i.e. the value of protected asset does not change and the level of this risk is only affected by the probability of the occurrence of negative event (security incident), we can also talk about **vulnerability analysis**.

It does not change the fact that the same principles are still used as are used in the risk analysis process.

Its means a combination of consequences and their likelihood of occurrence.

Co-funded by the
Erasmus+ Programme
of the European Union

Vulnerability assessment…

Risk		Possibility of occurrence <1-5>	<1-5>	Risk level
Event (scenario)	Consequence			
Theft of material from warehouse C2 outside working hours by climbing over the fence and breaking through the entrance door into the warehouse	Interruption of delivery of construction material to the production unit	4	5	20
Theft of material from warehouse C2 outside working hours by climbing over the fence and breaking through the window into the warehouse		4	5	20
Theft of material from warehouse C2 outside working hours by using a paraglider by entering via the roof ventilation system		1	5	5
Theft of material from warehouse C2 outside working hours by breaking through the perimeter wall that forms a part of the perimeter of the protected area		2	5	10

Co-funded by the Erasmus+ Programme of the European Union

Specific approaches…

There are three basic approaches to designing and evaluating the level of physical protection system which are used worldwide:

Directive approach where the subject must accept a precisely specified protection system regardless of its operation specifications and its environment.

Alternative approach where the subject can choose from a number of alternative solutions combining various protection measures.

Co-funded by the
Erasmus+ Programme
of the European Union

Specific approaches…

Flexible approach where the subject must accept those protection measures within the PPS which will take into account:

- resistance of mechanical barriers,
- response times of invervension units and
- probability of detection by alarm systems.

This approach is based on the premise: that the sufficient number of technical protection measures should be applied to detect and eliminate the intruder by the intervention unit before will achieve the goal (destroy, damage or still the protected assets).

Co-funded by the
Erasmus+ Programme
of the European Union

Specific approaches…

These three approaches can be generalized to two basic approaches: a quantitative and qualitative approach.

Qualitative approache where designing and evaluating PPS is based on expert estimations where the vulnerability of these systems cannot be precisely demonstrated and it is necessary to rely on the expertise of technical standards, legislations or software applications authors.

(e.g. RISKWATCH - Campus Security, RISKWATCH - Nuclear Power, RISKWATCH - Phys. & Homeland Security, RISKWATCH - NERC by Risk Watch International develops, USA).

Co-funded by the
Erasmus+ Programme
of the European Union

Specific approaches…

Quantitative approache is based on mathematical and statistical methods that enable exact demonstration of PPS vulnerability using measurable input and output parameters.

To be able to qualitatively determine protection level of any protected CI element or facility, it is necessary to create formalised description by a mathematical model.

Co-funded by the
Erasmus+ Programme
of the European Union

Specific approaches…

Examples of basic **input parameters**:

- breakthrough resistances of mechanical barriers,
- response time of intervention unit:
  - time of raising alarm,
  - time of attack verification,
  - transfer times of intervention units,
  - Intervention and elimination time,
- transfer times of intruder,
- time of intruder's attack,
- time of intruder's escape,
- probability of correct detection by the alarm system (e.g. PIR detector) in the detection zone during intruder

Co-funded by the
Erasmus+ Programme
of the European Union

Specific approaches…

- reliability of the alarm system,
- reliability of alarm signal transfer through the alarm transfer route to the alarm receiving centre,
- human factor reliability,
- probability of timely and correct evaluation of the alarm signal,
- alarm system detection characteristics,
- investment and/or operating costs.

Co-funded by the
Erasmus+ Programme
of the European Union

Specific approaches…

Examples of basic **output parameters**:

- effectiveness coefficient of protection measures,
- probability of eliminating the intruder (PI),
- cumulative probability of (correct) detection of the intruder.

Co-funded by the
Erasmus+ Programme
of the European Union

Specific approaches…

Example of software tools using quantitative approach:

- SAVI/ASSESS (Sandia National Laboratories, USA),
- Sprut (ISTA, Russia),
- Vega-2 (Eleron, Russia),
- Analizator SFZ (FRTK MFTI, Russia),
- SAPE (Korea Institute of Nuclear Non-proliferation and Control, South Korea)
- SatANO (the University of Žilina in Žilina, Slovakia).

Co-funded by the
Erasmus+ Programme
of the European Union

Software tools…

SAVI (Systematic Analysis of Vulnerability to Intrusion) is the first and best known SW tool for vulnerability evaluation of PPS.

This software has been designed to evaluate vulnerability of nuclear facilities protection systems and it is based on creation of deterministic routes and searching for the route with the least probability of interruption.

The **EASI** (Estimation of Adversary Sequence Interruption) model is used to calculate probability of interruption of a single route.

Co-funded by the
Erasmus+ Programme
of the European Union

Software tools…

The whole system is describe by the **ASD** diagram (Adversary Sequence Diagram).

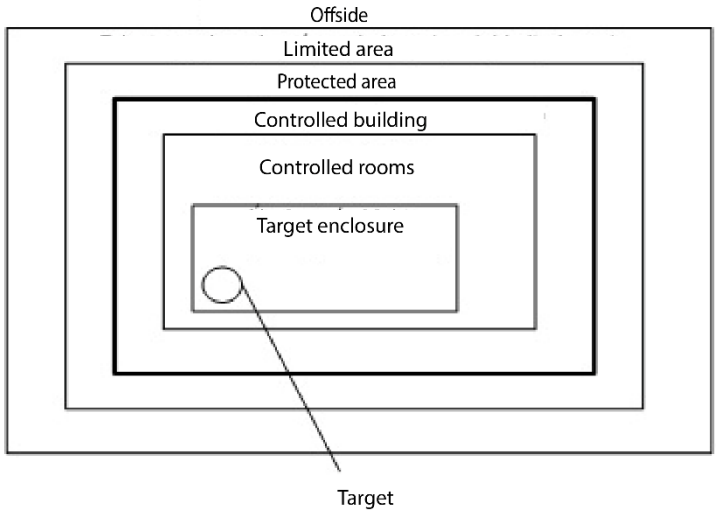
ASD represents a method to graphically present possible attack routes within the PPS.

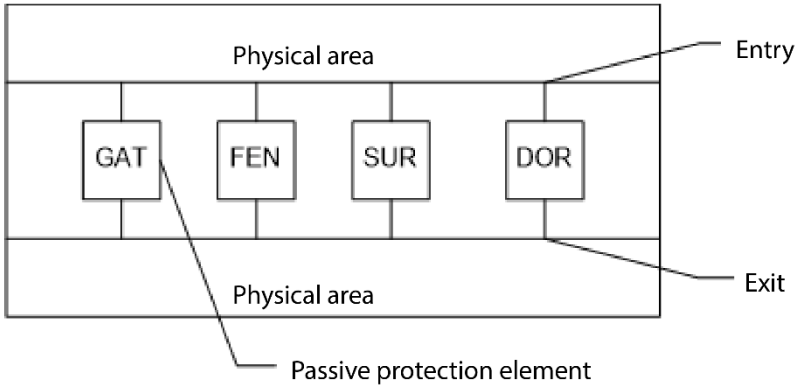
SAVI creates a list of the ten most vulnerable routes in terms of probability of interruption.

SAVI is supplemented with an large database of delay and detection parameters of the most commonly used protection measures.

Co-funded by the
Erasmus+ Programme
of the European Union

Software tools…





ASD diagram modelling

Co-funded by the
Erasmus+ Programme
of the European Union

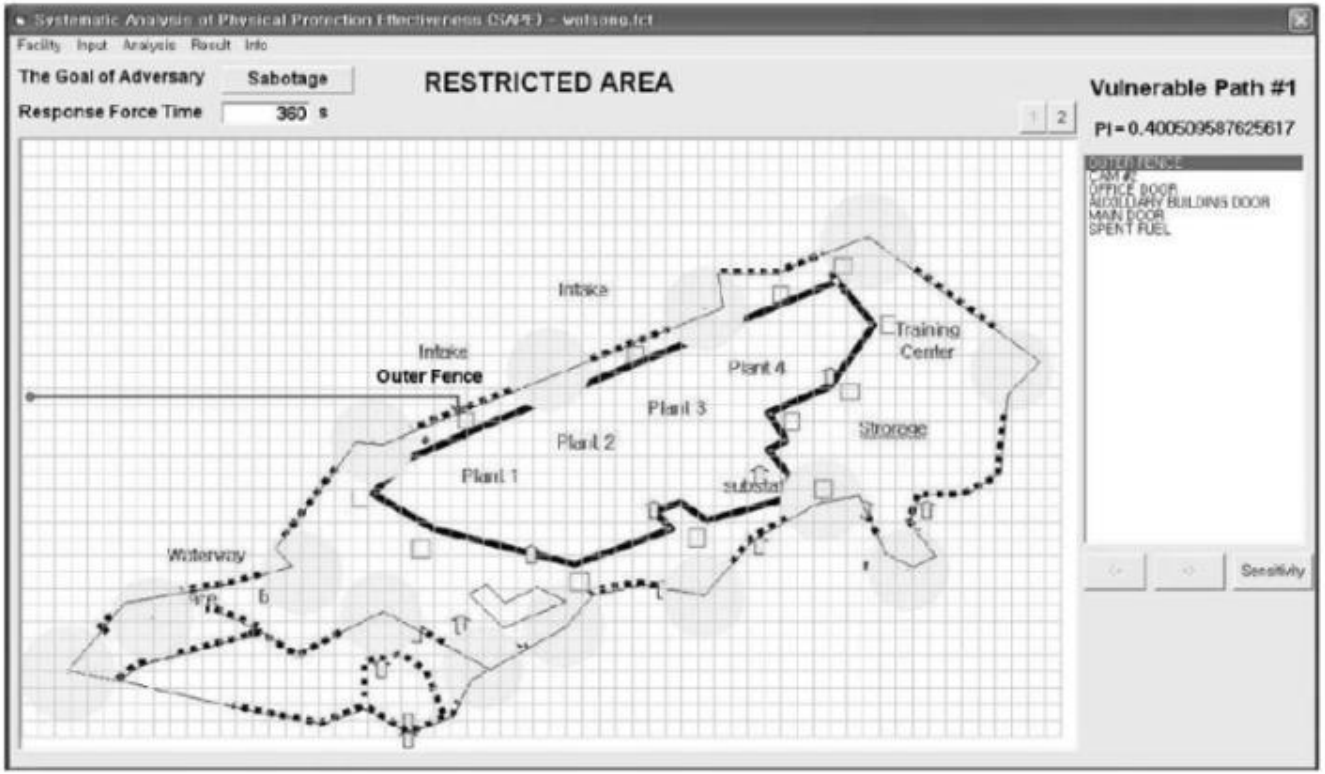
Software tools…

SAPE (Systematic Analysis Of Physical Protection Effectiveness - Korea Institute of Nuclear Non-proliferation and Control) is a software tool for vulnerability evaluation of PPS which is based on SAVI and ASSESS but is significantly enhanced.

SAPE substitutes the ASD method by a two-dimensional maps since the ASD diagram is sometimes unclear.

Co-funded by the
Erasmus+ Programme
of the European Union

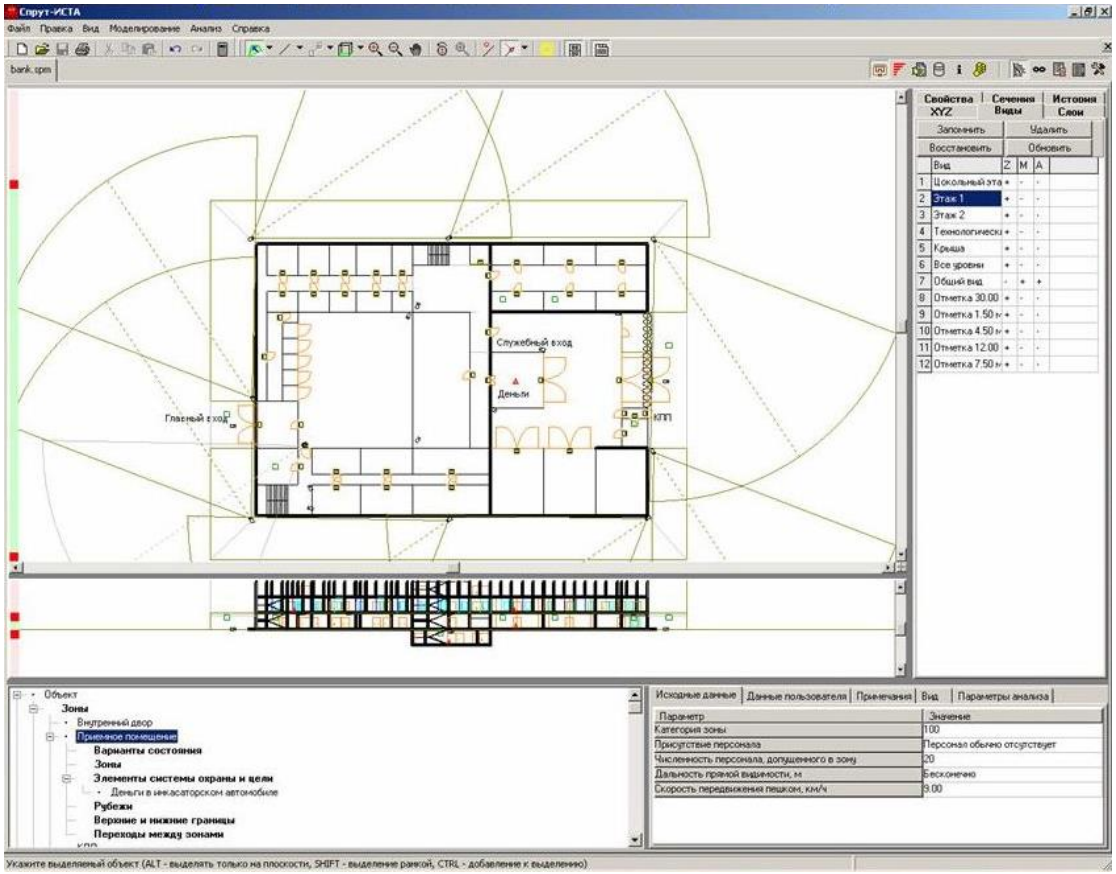
Software tools…



SAPE Graphical User Interface

Co-funded by the
Erasmus+ Programme
of the European Union

Software tools…



SPRUT Graphical User Interface

Co-funded by the
Erasmus+ Programme
of the European Union

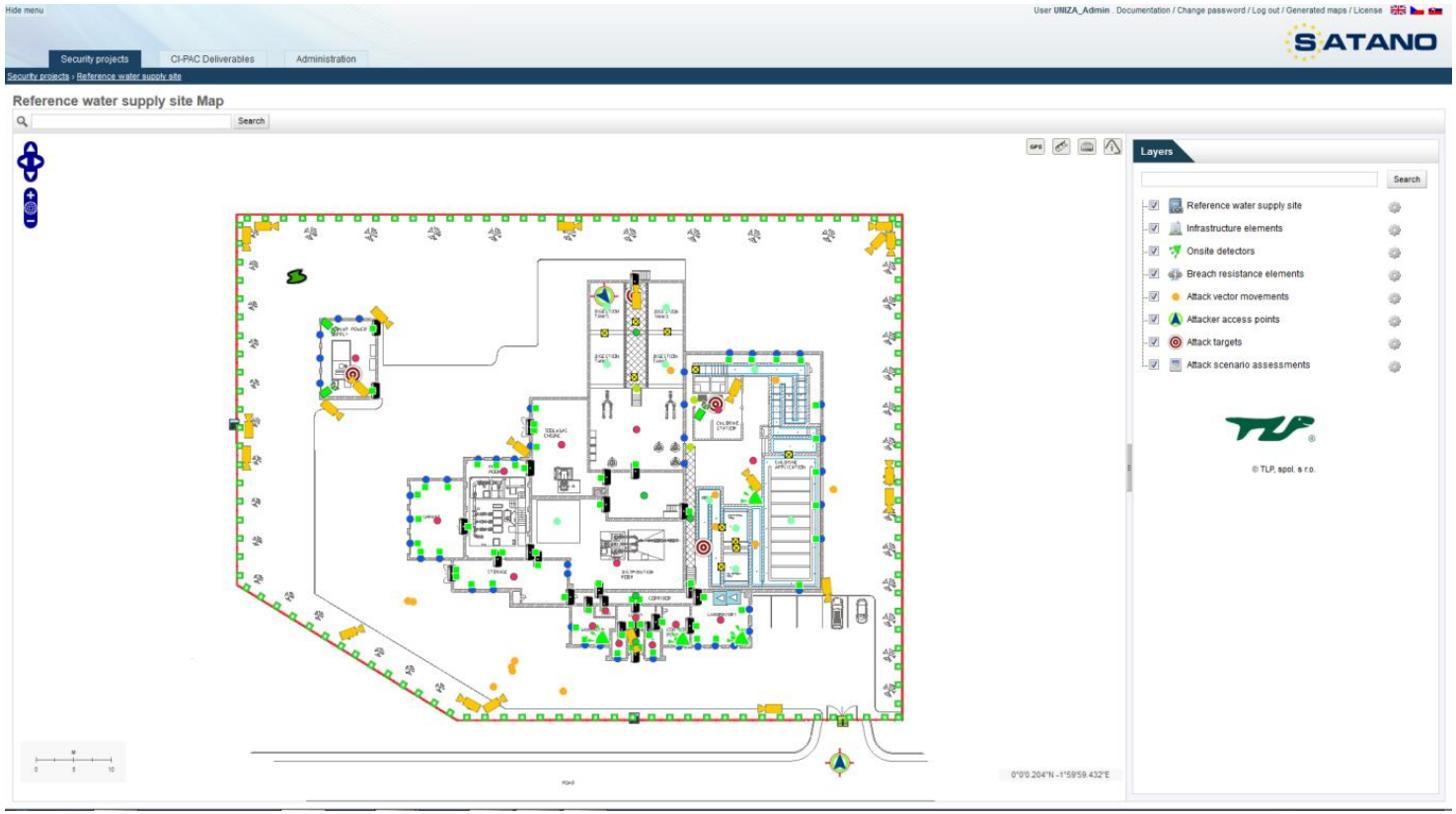
SATANO Software tools…

The Security Assessment of Terrorist Attack in a Network of Objects (SATANO) is a new simulation tool enabling the quantitative assessment of the level of PPSs for critical infrastructure elements using various 2D maps.

This software was created as part of the Critical Infrastructure Protection Against Chemical Attack (CI-PAC) project (HOME/2013/CIPS/AG/4000005073), undertaken between 2014 and 2016.

Co-funded by the
Erasmus+ Programme
of the European Union

SATANO Software tools…



SATANO Graphical User Interface

Co-funded by the
Erasmus+ Programme
of the European Union

SATANO Software tools…

The SATANO software tool using the flexible approach based on the premise that that the sufficient number of technical protection measures should be applied to detect and eliminate the intruder by the intervention unit before will achieve the goal (destroy or damage protected assets).

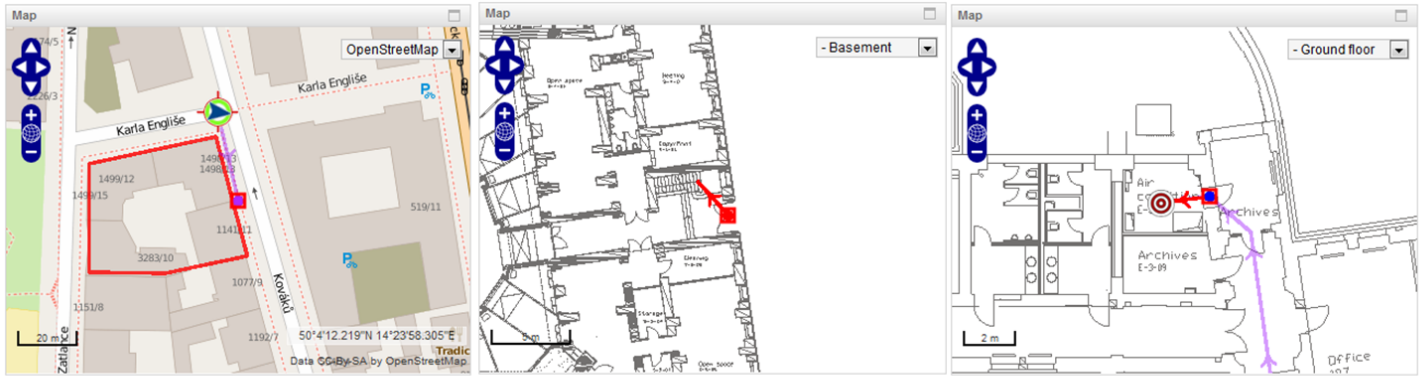
SW calculate with hypothesis that the intruder have all the necessary information about the protected interest.

He makes a decisions at certainty and knows the critical path/route.

Co-funded by the
Erasmus+ Programme
of the European Union

SATANO Software tools…

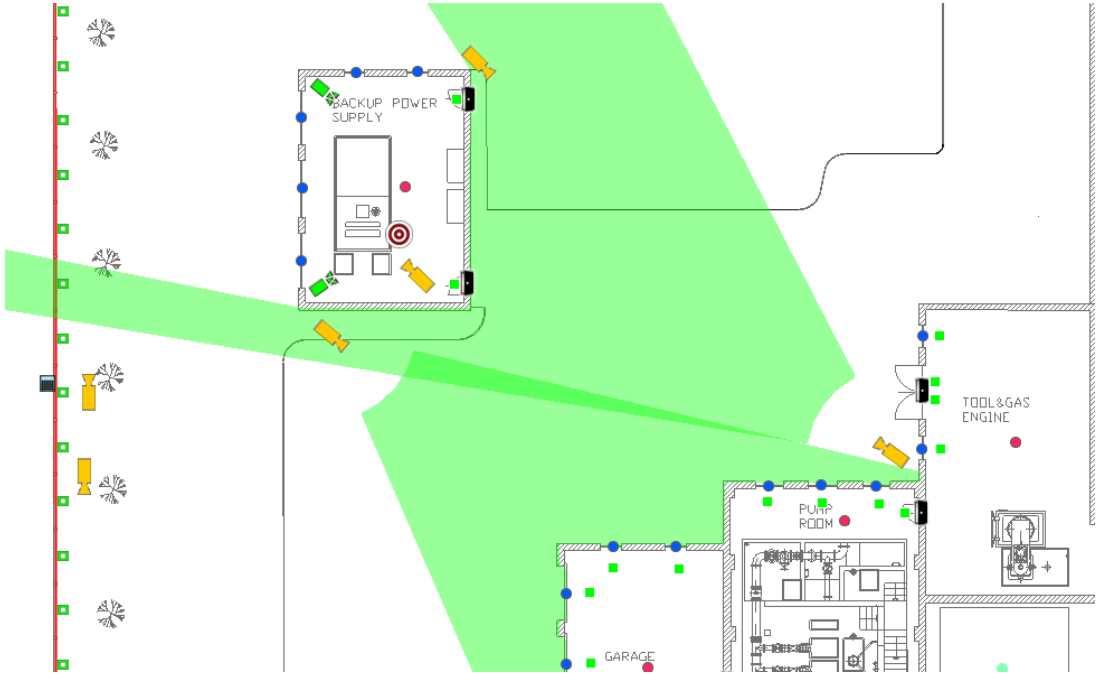
Its possible to model the system of physical protection using various map in a relevant scale. This tool, unlike other software tools (e.g., SAVI), is suitable for any multi-storey building or line construction, etc. (e.g., airports, administration buildings, oil pipelines, and water supply sites).



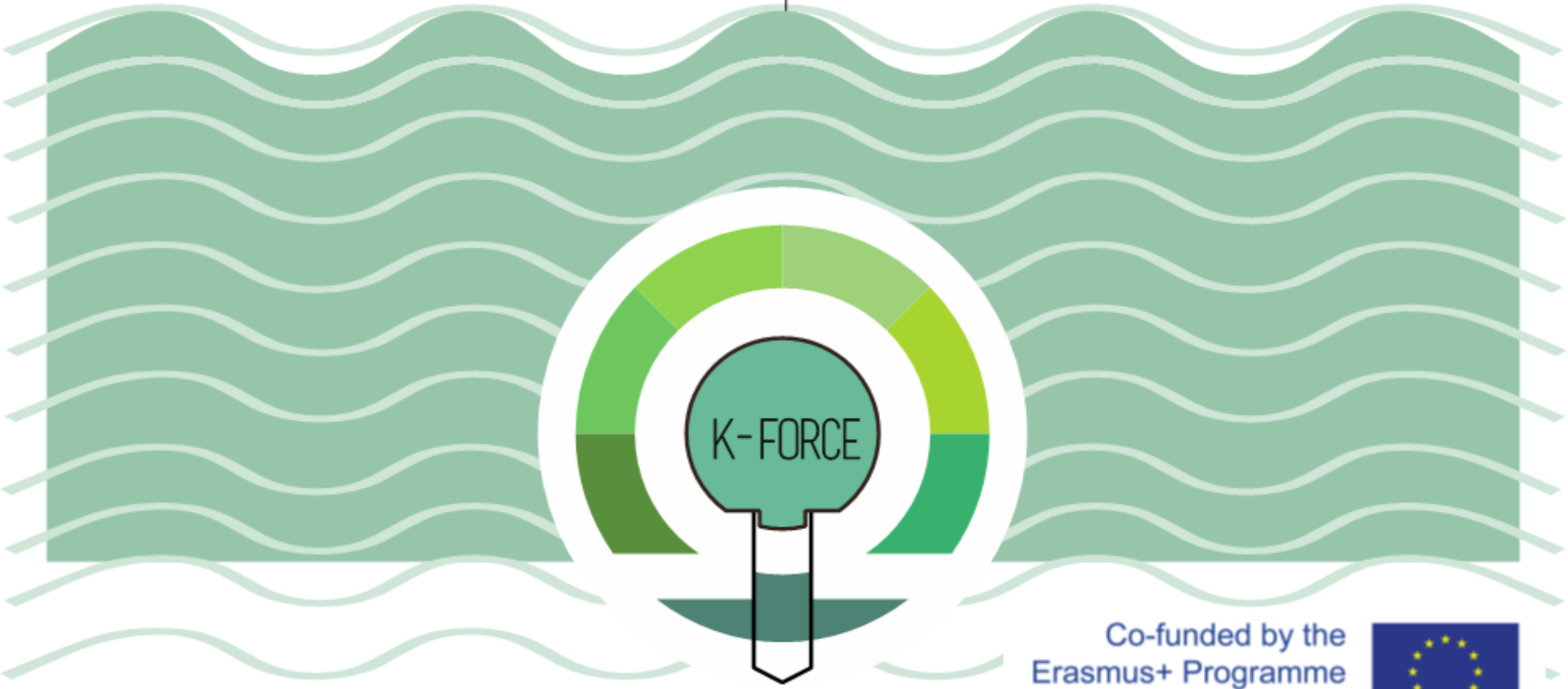
Co-funded by the
Erasmus+ Programme
of the European Union

SATANO Software tools…

It is also able to model detection zones depending on the alarm system's parameters (e.g., the intruder detection system, camera surveillance system).



Co-funded by the Erasmus+ Programme of the European Union



Co-funded by the
Erasmus+ Programme
of the European Union

Thank you
for your attention

Tomas.Lovecek@fbi.uniza.sk

Knowledge **FO**r **R**esilient so**C**i**E**ty