

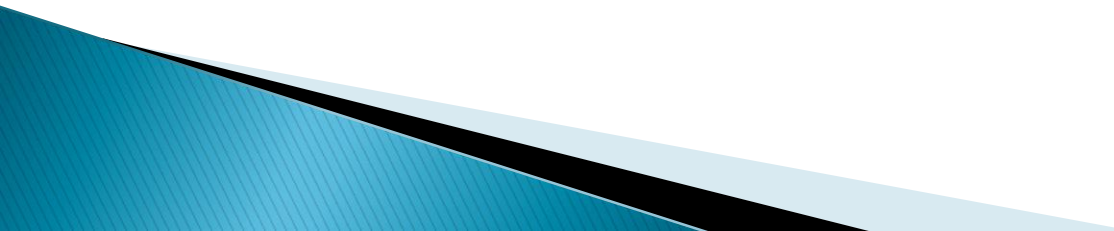


Critical infrastructure protection and resilience – theory and practise

Martin Hromada

DEPARTMENT OF SECURITY ENGINEERING
FACULTY OF APPLIED INFORMATICS
TOMAS BATA UNIVERSITY IN ZLIN
HROMADA@FAI.UTB.CZ

Agenda

1. Critical Infrastructure
 2. Critical Infrastructure in Czech Republic/Energy Sector
 3. Knowledge sharing concept
 4. RISK Analysis
 5. Physical Protection Systems
 6. Physical Protection Systems Functionality Evaluation – EASI MODEL
 7. Risk scenario exercise
 8. Critical infrastructure resilience assessment
- 

Motto:

▶ *When we flip a switch, we expect light. When we pick up a phone, we expect a dial tone. When we turn a tap, we expect drinkable water.*

Critical Infrastructure

- Critical infrastructure' means an asset, system or part thereof located in Member States which is essential for the main-tenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions;
- Critical infrastructure is complex of critical infrastructure sectors, whose destruction or disturbance has significant consequences to basic society functions, health, defence, security and occupant life quality from economical and social point of view.

Critical Infrastructure

- ▶ European critical infrastructure' or 'ECI' means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure;

Critical infrastructure protection

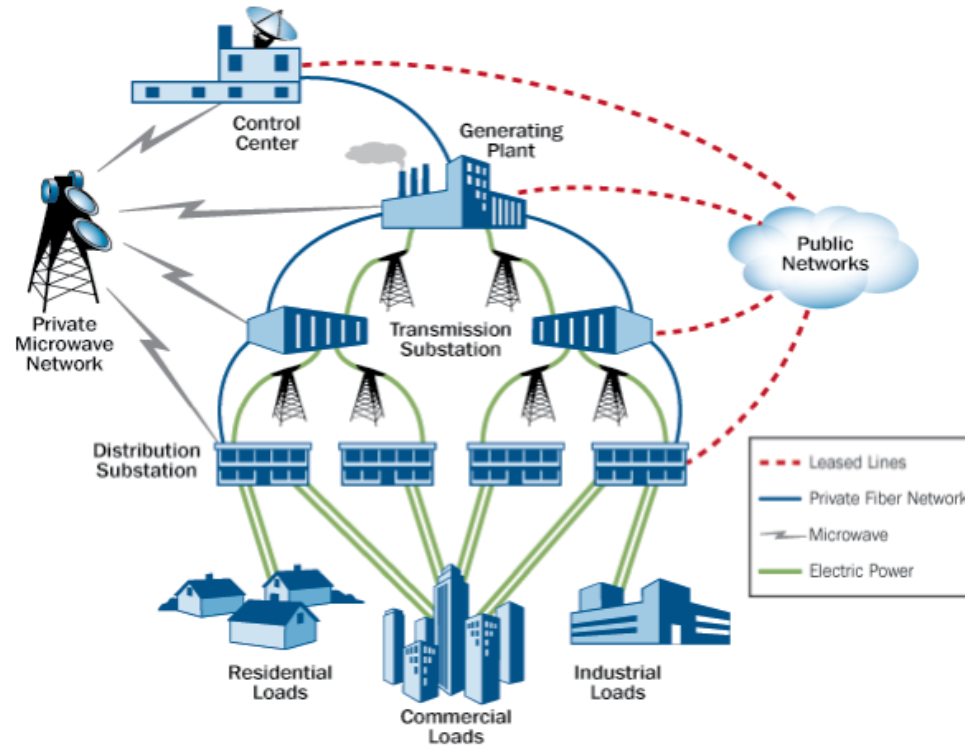
Council Directive 2008/14/ES on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection

- ▶ Operator security plan OSP
- ▶ Security Liaison Officer SLO
- ▶ European Critical Infrastructure Protection Contact Points ECIP

Non – Binding Guidelines, for application of the Council Directive

- ▶ Cross – cutting criteria
 - Casualties criterion
 - Economic effect criterion
 - Public effect criterion
- ▶ Sector criteria

Critical Infrastructure in Czech Republic/Energy Sector



Critical Infrastructure in Czech Republic/Energy Sector

Electricity

A1 production site of electricity

- a) Production site with a total installed power output of at least 500 MW,
- b) Production site providing supporting services with a total installed power output of at least 50 MW or with their activations within 15 minutes,
- c) Wiring for power transmission for securing their own electricity generating stations,
- d) Electricity producers dispatching.

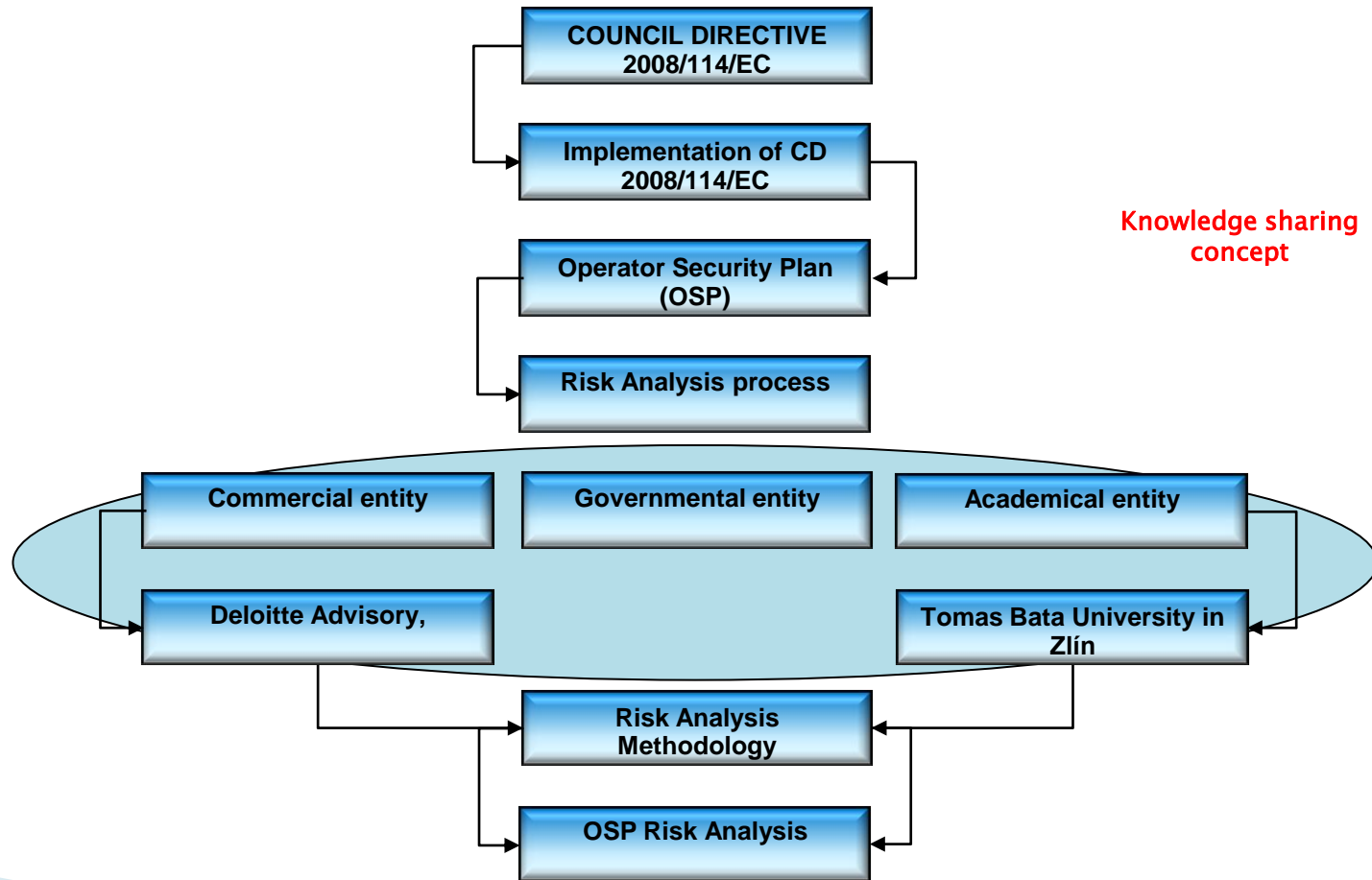
A2 the transmission grid

- a) transmission system with a voltage of 110 kV,
- b) the electrical transmission system station with a voltage of 110 kV,
- c) technical dispatching of the transmission system operator.

A3 Distribution System

- a) and electrical distribution system station with a voltage of 110 kV (station type 110/22 kV and 110/35 kV shall be assessed according to their strategic importance in the distribution system),
- b) Technical dispatch) the distribution system operator.

Knowledge sharing concept

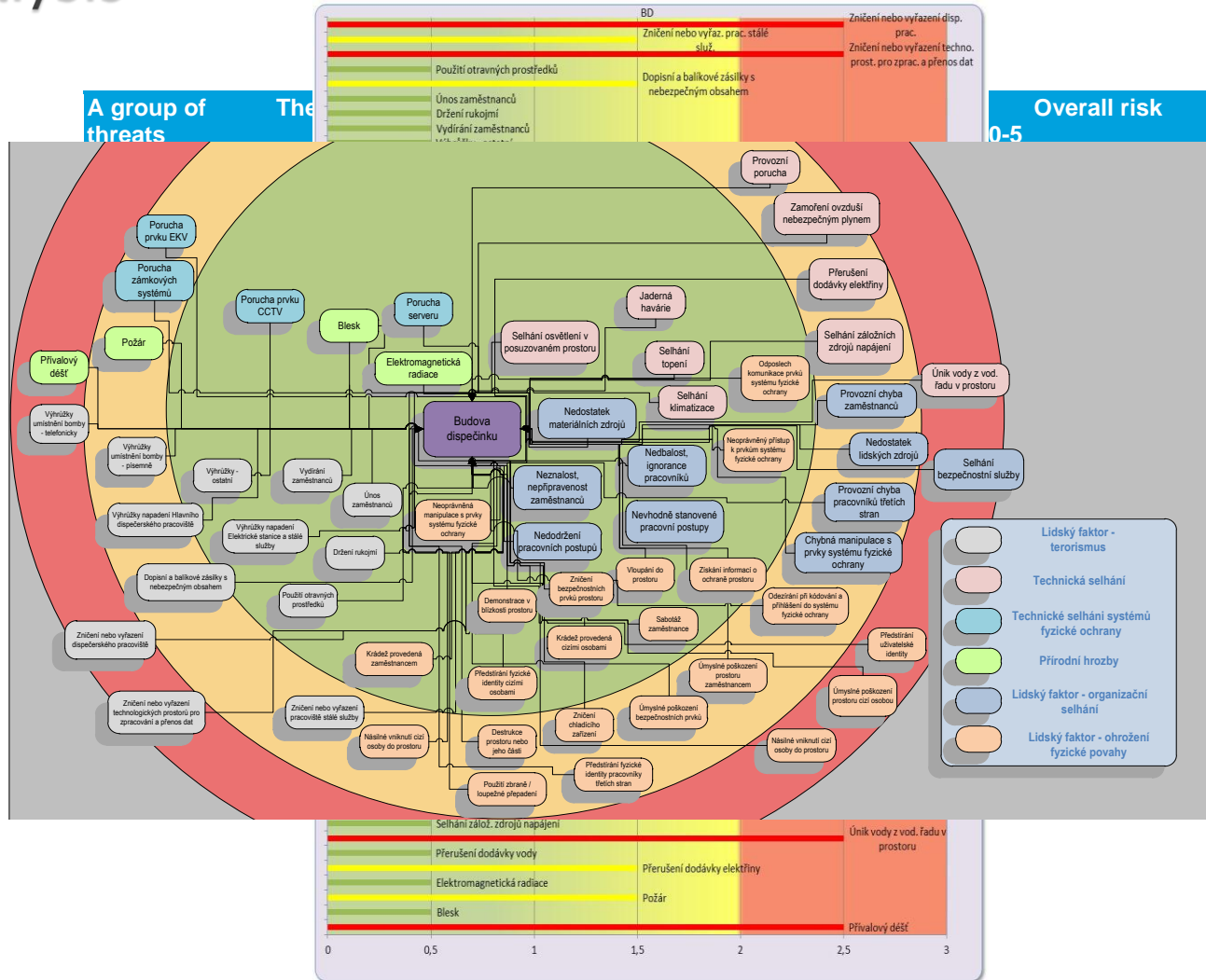


RISK Analysis

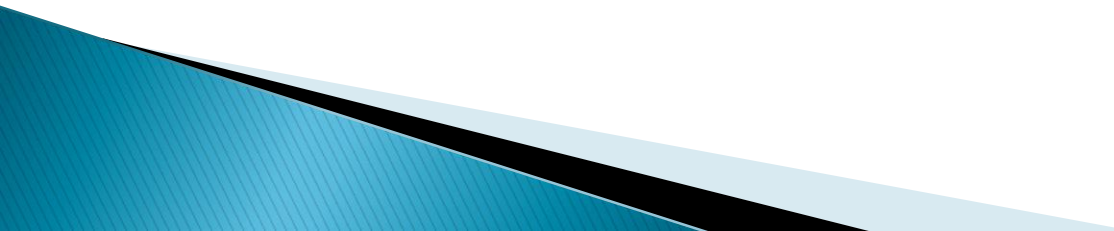
- For optimal expression of security measures is necessary to establish the scope and framework for a comprehensive risk assessment of identified assets.
- Risk evaluation in the particular area is expressing and evaluating vulnerability, which is perceived as an expression of a weak spot in the system
- The value alone will be based on current attitudes of quantitative risk formulation, which means that the risk value will be a numerical expression of product of assets numerical value, threat and vulnerability according to a relation:
 - ▶ R – risk
 - ▶ A – asset value
 - ▶ T – threat
 - ▶ V – vulnerability

$$R = A \times T \times V$$

RISK Analysis



RISK Analysis

- In risk and vulnerability assessment process is necessary to use relevant methodology for the expression of the mutual relationships and interdependencies between identified risks. For this purpose, the QARS (Qualitative risk correlation analysis) methodology was selected.
 - The importance of this method is especially in connection with the diversification of risk based on level of risk activity (the risk ability or potential to cause further risks) and passivity (possibility that the risk may be caused by other risks) in relation to other risks.
- 

RISK Analysis

- The process of implementation of the QARS analysis is multi-steps process, where in the first step the list of risk is created. The next step is focused on the expression of importance relations and interdependencies between the identified risks in the form of spreadsheet correlation.

Index		1	2	3	4
Index.	The Threat Of	High temperature	Lightning	Tree fall	Operating error of third parties
1	High temperature	x			
2	Lightning	1	x	1	0

- ▶ x – Reflects the fact that the risk itself cannot cause,
- ▶ 1 – Is the real possibility that the risk R_i may cause risk R_j ,
- ▶ 0 – Expresses a condition where there is no real possibility that the risk R_i may cause risk R_j

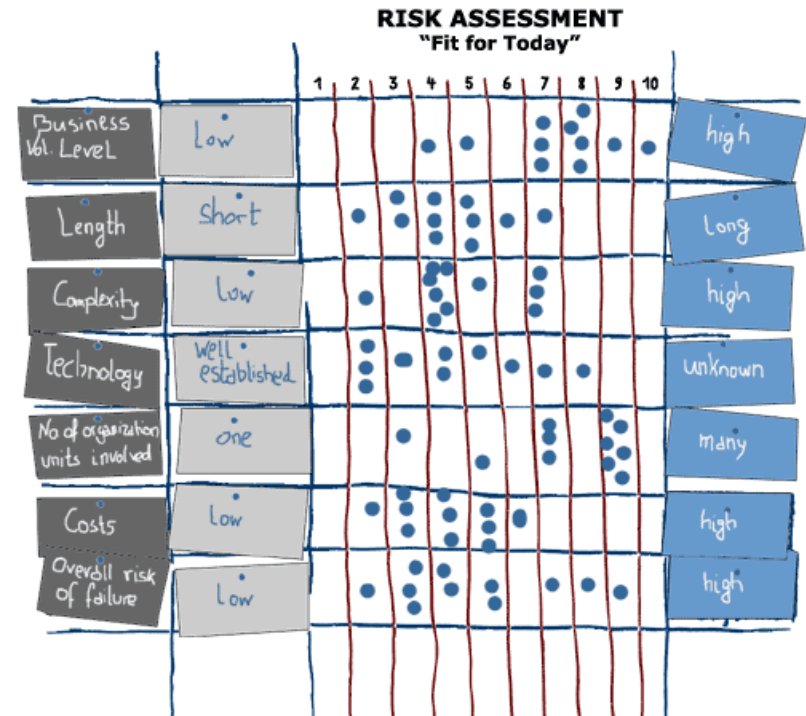
RISK Analysis

- ▶ To calculate the coefficients of the relationships and interdependencies we apply:

$$C_A R_i = \frac{\sum R_i}{x-1}$$

$$C_P R_i = \frac{\sum R_i}{x-1}$$

- ▶ where:
- ▶ $C_A R_i$ is the value of activity coefficient,
- ▶ $C_P R_i$ is the value of passivity coefficient,
- ▶ $\sum R_i$ is the sum of risks,
- ▶ x - total number of risk,



RISK Analysis

- After adding values to the correlation table, the horizontal axis (activity coefficient) and vertical axis (passivity coefficient) after using equations has following parameters:

The Risk Index		1	2	3	4	5	6	7	8	9	10
Activity Coef.		0,00	0,22	0,44	0,44	0,56	0,56	0,67	0,56	0,11	0,11
Passivity Coef.		0,67	0,00	0,11	0,44	0,67	0,00	0,44	0,33	0,44	0,33

- Subsequently, the values were plotted in the graph, which ultimately enables the most significant risks assessment in term of its potential (high activity and passivity potential).

RISK Analysis

- For the risk assessment or for the process of determining the most significant risks, must be the graph divided into segments that diversify risks according their significance. To divide the graph into 4th segments is necessary to define S1 and S2 lines that divide the graph itself and the risks to the segments where it is assumed that in the first segment will be 80% if major risks.
- To express the parameters for line S1 and S2 we use the equations:

$$S_{1/2} = C_{A/P\max} - \frac{(C_{A/p\max} - C_{A/P\min})}{100} * 80$$

where:

- ▶ $C_{A\max} ; C_{A\min}$ Minimum and maximum values of activity coefficient,
- ▶ $C_{P\max} ; C_{P\min}$ Minimum and maximum values of passivity coefficient

RISK Analysis

- ▶ From the previous table we express the maximum and minimum values for individual coefficients:

The Risk Index		1	2	3	4	5	6	7	8	9	10
Activity Coef.		0,00	0,22	0,44	0,44	0,56	0,56	0,67	0,56	0,11	0,11
Passivity Coef.		0,67	0,00	0,11	0,44	0,67	0,00	0,44	0,33	0,44	0,33

- ▶ C_{Amax} – 0.67
- ▶ C_{Amin} – 0.11 – for better accuracy we calculated values out of 0
- ▶ C_{Pmax} – 0.67
- ▶ C_{Pmin} – 0.11 – for better accuracy we calculated values out of 0

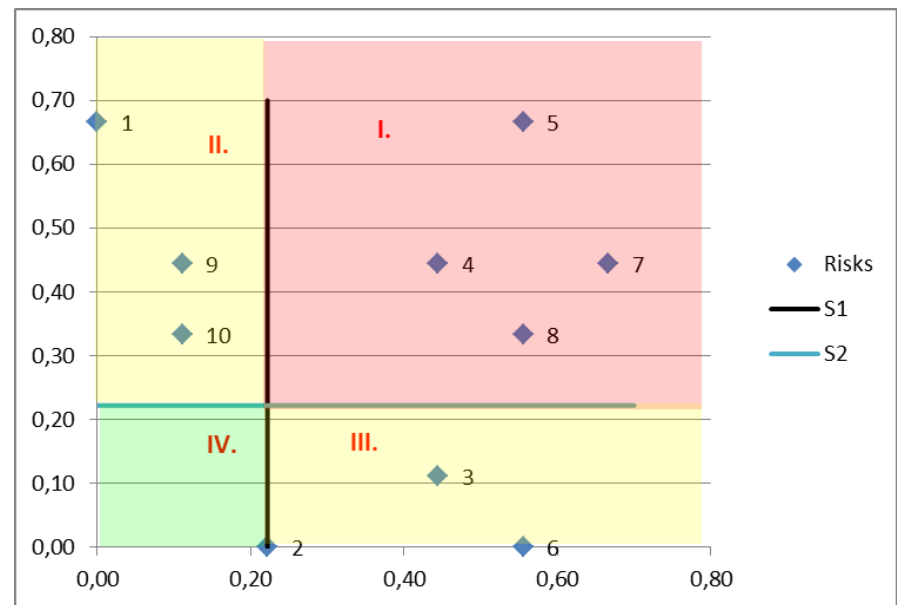
- ▶ Substituting into the equation for calculation of S1 and S2:

$$S_1 = 0,67 - \frac{(0,67 - 0,11)}{100} * 80 = 0,22$$

$$S_2 = 0,67 - \frac{(0,67 - 0,11)}{100} * 80 = 0,22$$

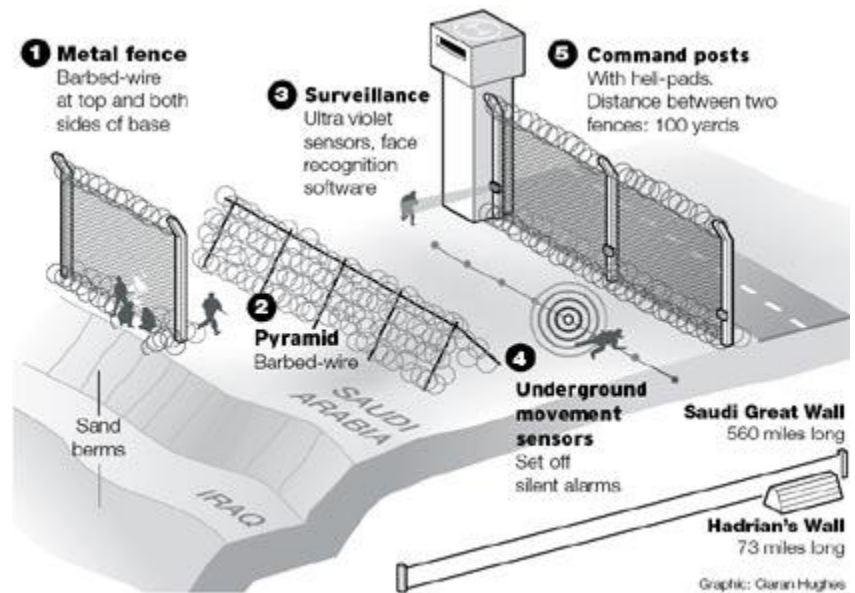
RISK Analysis

- Then the lines are implemented into the graph and we divide the risks by 4 segments that represent the level of risks:
- I. Segment – Primarily significant risks – the highest activity and passivity coefficients,
- II. and III. Segment – Secondary significant risks,
- IV. Segment – Tertiary significant risks – low value of activity and passivity coefficients,



Physical Protection Systems

- Physical protection is secured by companies in the commercial security industry (CSI). In CSI, the physical protection of any object (building, appliance, object etc.) is achieved by combining and intertwining of three basic elements: System of technical protection systems, response team/activity, regime protection:
- Mechanical barrier systems
- Intrusion & Hold-up alarm systems
- Response team/activity
- Regime protection/measure



Physical Protection Systems

- Mechanical barrier systems – in object concepts as the building are walls, roofs, floors, doors and windows objects. Generally these are for example: security locks, grilles, security film, security and toughened laminated glass, safe, safety deposit boxes...



Physical Protection Systems

- Mechanical barrier systems – are defined as systems or devices that are designed to prevent unauthorized access. These systems can include:
 - Perimeter protection (fixed barriers, fences, sensor guards, gates, barriers, turnstiles, security gates and others);
 - Shell protection (grilles, shutters, follies, blinds, safety glass, windows, doors, door frames, walls, locks, lock cylinders, padlocks and other),
 - Object protection (strong-rooms, commercial storage units and others).



Physical Protection Systems

- Intrusion and/or Hold-up Alarm System (I&/orHAS); Security Camera System (CCTV system, CCTV surveillance system); Fire alarm system (FAS); Access Control System (ACS); Mechatronics System.



Physical Protection Systems

For technical security means can be considered:

- systems for access control,
- the alarm systems for reporting violations,
- the camera systems in a closed television circuit,
- electrical fire alarm,
- facilities for detection of substances and articles
- the device against active eavesdropping,
- the device for physical destruction of information,
- the emergency systems.



Physical Protection Systems

- Response team/activity – can be carried out by own resources, security, private security service employees or by police or army. This type of protection is expensive but very active and effective. The core is a response of a human element to impulses related to danger / security disruption / object protection such as. breaking in, technological breakdown etc. Impulses for a response team reaction are carried out by an I&HAS.



Physical Protection Systems

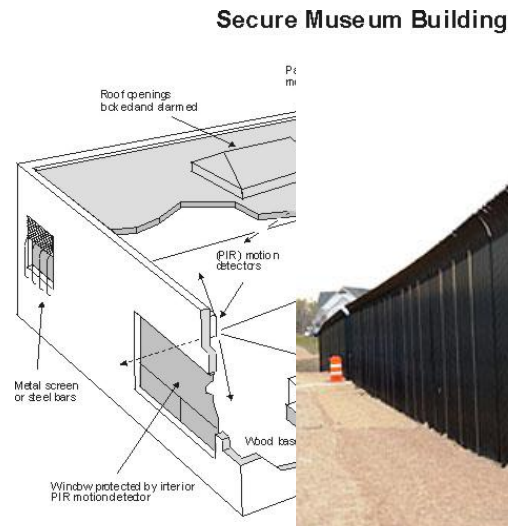
Regime protection/measure – consists of a compilation of administrative and organization measures for securing protected interests and values. Generally considered the most important are:

- a) Input and output mode of persons and means of transport which includes namely checking the entrance of employees, clients, visitors and foreigners into the object and its parts, checking the leaving of persons and vehicles from the object, a right to take out objects and materials.
- b) Mode of the employee's movement in the object which also includes a determination of a part of an object with limited accessibility for employees and designation of their affiliation to certain transports, working places etc.
- c) Material and expedition mode sets the procedure when receiving, storing, exporting and movement of material. This way the property is protected against theft, damage and devaluation

Physical Protection Systems Design

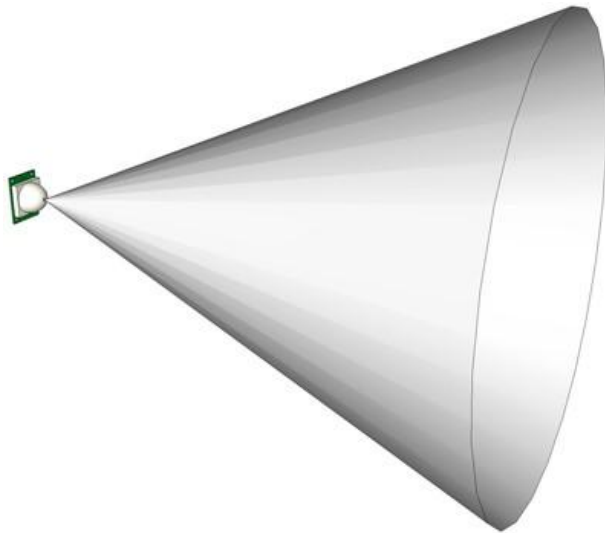
In order to articulate the optimal system structure and functionality of the physical protection system of the critical infrastructure element, it is necessary to define the key functions of the system and its sub-systems. In association with the comprehensive utilization of the physical protection system, three main system functions and its sub-systems parameters are considered:

- a) Detection
- b) Delay
- c) Response



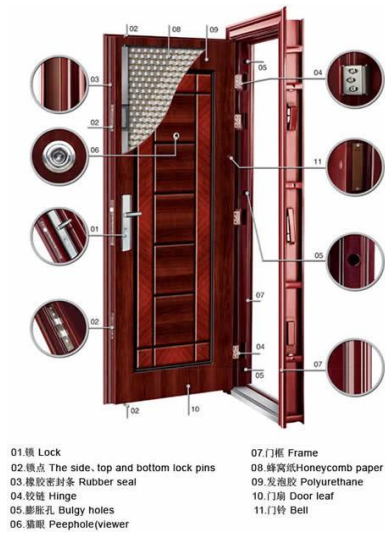
Physical Protection Systems Design

- Detection – detection of an adversary with the use of technical security devices (AIR, PIR, MW Bistatic, MW Monostatic, dual sensor, etc.) and verification of the alarm information via the closed-circuit television (CCTV); parameter – probability of detection, the time needed for the verification of alarm information and probability of successful communication.



Physical Protection Systems Design

- Delay- hindering of the adversary with the mechanical barrier systems application (fences, gates, barriers, grids, security doors, glass and other); parameter - breaking resistance
- Response - the response of the object's guards - preventing or interrupting the activity of the adversary or his arresting even with the use of regime measures; parameter - the time needed for the guards to transfer from A to B



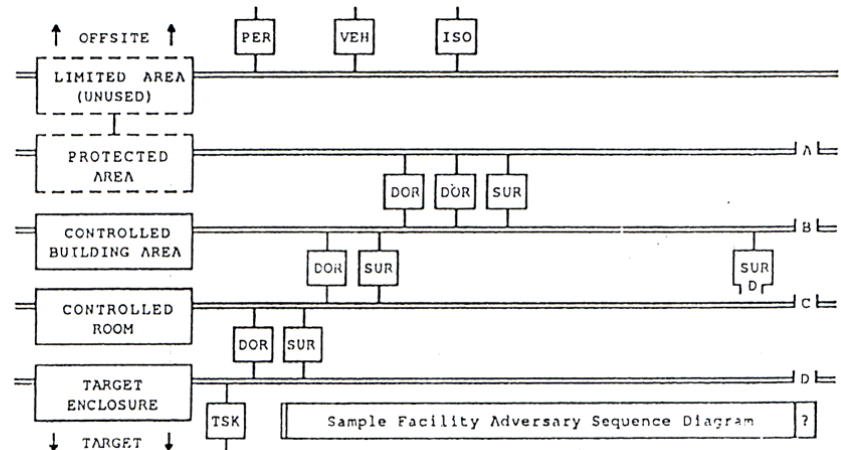
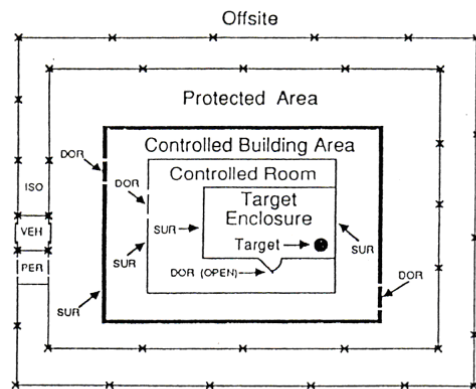
Physical Protection Systems Functionality Evaluation

EASI, ASD, SAVI (SANDIA NATIONAL LABORATORIES, USA)

- These three closely interconnected methods are based on detection of path with lowest cumulative probability of detection up to critical point of detection and are intended for evaluation of nuclear facility security technical effectiveness. They utilize central division of security zones with one zone containing protected asset in middle of whole system and are based on intruder's familiarity with the security system.
- According to terminology used in these methods the path with lowest cumulative probability of detection up to critical point of detection is called critical path or path with lowest cumulative probability of interruption. Detection before critical point of detection is called timely detection.

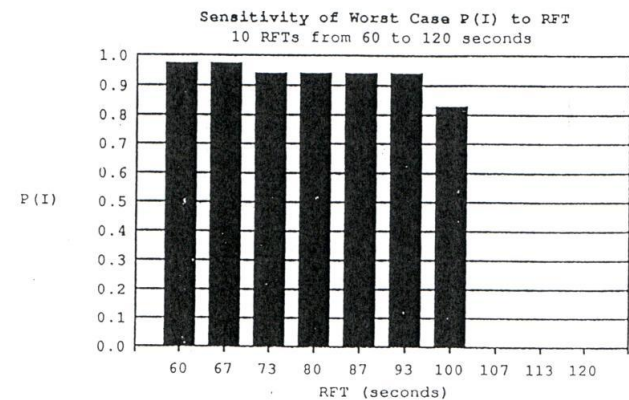
Physical Protection Systems Functionality Evaluation

- EASI method (Estimation of Adversary Sequence Interruption) allows calculation of interruption probability only on one predefined path.
- ASD Method (Adversary Sequence Diagram) is method for graphic representation of possible intruder paths in security system.
- ASD describes facility and its security system as layers that separate external intruder from his target inside facility. Individual physical areas are separated by protective barriers that include everything that may delay or detect intruder.



Physical Protection Systems Functionality Evaluation

- SAVI method (Systematic Analysis of Vulnerability to Intrusion) combines EASI and ASD methods and evaluates every possible path to central zone from the viewpoint of interruption probability, and creates list of ten most vulnerable paths according to their possibilities of interruption. If values of interruption probability are equal, it lists paths according to total length of attack. Main SAVI program is accompanied by extensive database of delay and detection parameters of most commonly used protection elements.
- SAVI method implements also sensitivity analysis. Given that most critical parameter is time required for response, for sensitivity analysis SAVI uses different values of response team time. Output is interruption probability. Figure 4 shows sensitivity analysis for path with lowest interruption probability.



Physical Protection Systems Functionality Evaluation – EASI MODEL

- According to the above, structural assessment of the physical protection system lacks assessment of its functionality which specifies both the relation between the activity of the adversary and the response team and at the same time takes into account and utilizes the dependencies that emerge from basic structure and functionality demands and main system functions, which has been presented in the previous slides. These dependencies may also be expressed by this relation:

$$P_D = P_S * P_T * P_A$$

- ▶ PD – Probability of detection,
- ▶ PS – Probability of detection ability,
- ▶ PT – Probability of successful transfer,
- ▶ PT – Probability of successful assessment,

Physical Protection Systems Functionality Evaluation – EASI MODEL

- The model assesses and works with already determined parameters of the physical security system components where the outcome is estimation of adversary sequence interruption which is today used by National laboratories, Sandia USA and was published by M. L. Garcia, The Design and Evaluation of Physical Protection Systems, 2007.

Estimate of Adversary Sequence Interruption

Probability of Guard Communication		Response Force Time (in Seconds)	
0.97		Mean	Standard Deviation
		172.8	78.8

Task	Description	P(Detection)	Location	Delays (in Seconds):	
				Mean	Standard Deviation
1	Zone 1	0.9	I	25.5	9.2
2	Zone 2	0.9	I	75	22.5
3	Zone 3	0.9	I	113.4	32.6
4	Zone 4	0.9	I	285	85.5
5	Zone 5	0.9	I	77.7	22.1
6	Zone 6	0.9	I	285	85.5
7	Zone 7	0.9	I	17.1	4.1
8	Zone 8	0	I	0	0
9					
10					
11					
12					

Probability of Interruption: 0.969935157

Estimate of Adversary Sequence Interruption

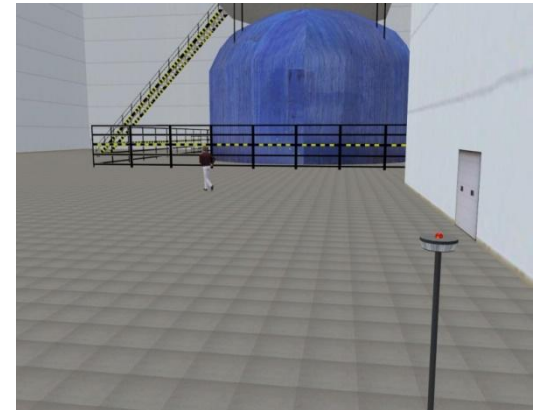
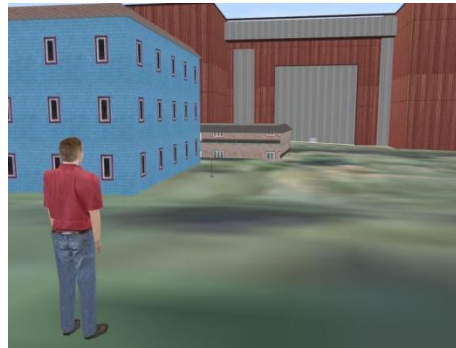
Probability of Guard Communication		Response Force Time (in Seconds)	
0.998		Mean	Standard Deviation
		172.8	78.8

Task	Description	P(Detection)	Location	Delays (in Seconds):	
				Mean	Standard Deviation
1	Zone 1	0.95	IV	25.5	9.2
2	Zone 2	0.95	IV	170	51
3	Zone 3	0.95	IV	113.4	32.6
4	Zone 4	0.95	IV	890	267
5	Zone 5	0.95	IV	77.7	22.1
6	Zone 6	0.95	IV	895	268.5
7	Zone 7	0.95	IV	17.1	4.1
8	Zone 8	0.95	IV	955	286.5
9					
10					
11					
12					

Probability of Interruption: 0.997999997

Physical Protection Systems Functionality Evaluation

- In order to raise the EASI outputs relevance and value of estimate of adversary sequence interruption in the object, it is necessary to simulate the movement of the adversary and response team with a simulation tool which works with parameters specified for the EASI model and with real conditions.
- In this context, the OTB SAF simulation tool (OneSEMI–Automated Forces Testbed /OneSAF Testbed Baseline; Science Applications International Corporation San Diego California USA; national representative Lynx Ltd. Košice), in which a physical protection system was built-in for critical infrastructure elements physical protection system functionality assessment and EASI model outputs verification.



Physical Protection Systems Functionality Evaluation – OTB SAF

- For physical protection system penetration approach and functionality assessment, the reference object was created – power plant with control points (checkpoints) created a potential points of mechanical barrier systems disturbance.



Physical Protection Systems Functionality Evaluation

- The critical infrastructure element physical protection system penetration tests were carried out in the referential object. These tests were also considered to be a form of the EASI model verification.
- According to the carried-out simulations, the EASI model is, in the context of verification of the physical protection systems functionality, an applicable model. This is in relation to potential purloin or destruction of the protected interest in terms of the critical infrastructure element.

Number of zones overcome	EASI model output – estimate of adversary sequence interruption	EASI model simulation verification via OTB SAF tool
0	0,9699352	1
1	0,9693818	1
2	0,9640465	1
3	0,9137656	1
4	0,7589453	1
5	0,0223934	0
6	0,0123595	0
7	0,0000000	0
8	0,0000000	0



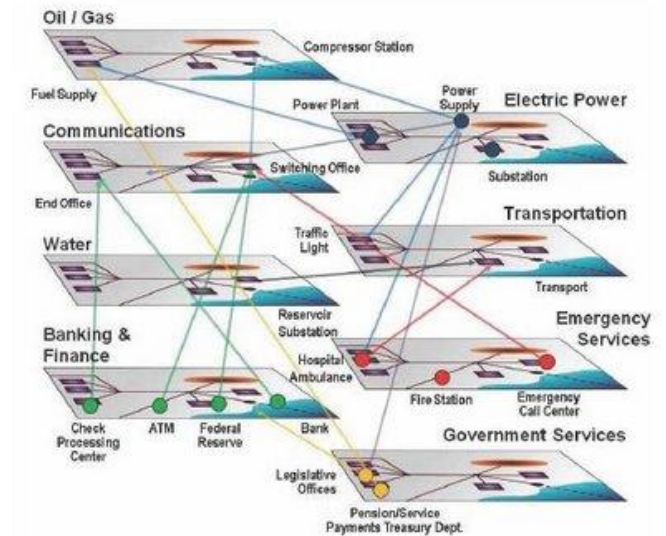
Resilience assessment – terminology definition

- ▶ *'critical infrastructure'* means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions,
- ▶ *'resilience'* is understood „The ability of systems, infrastructures, government entities, businesses, and society to adapt to adverse events, to minimize the impact of such events (keeping the system running), and also to anticipate future adverse events and be able to prevent them

Indicators for Resilience Evaluation

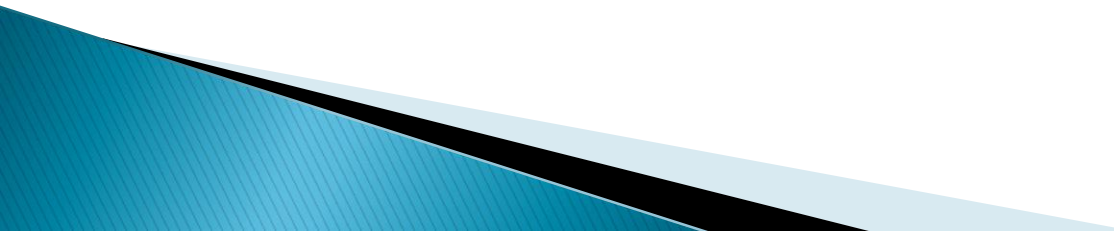
In context of resilience evaluation the basic indicators are:

- ▶ robustness,
- ▶ preparedness,
- ▶ responsiveness,
- ▶ recoverability.



Procedures and Phases of Critical Infrastructure Resilience Evaluation

Evaluated Critical Infrastructure Element System Analysis,

- ▶ Risk Assessment and Analysis,
 - ▶ Determination of the Resilience Attributes and Indicator Values,
 - ▶ Calculation of Critical Infrastructure Element Resilience for Selected Risk,
 - ▶ Final Critical Infrastructure Element Resilience Evaluation.
- 

Procedures and Phases of Critical Infrastructure Resilience Evaluation

Evaluated Critical Infrastructure Element System Analysis

- ▶ Main/objective function (output, product, service) of evaluated object (s)/critical infrastructure elements,
- ▶ procedural or functional architecture, presenting an overview of key processes that ensure the element target function (specify the characteristics of processes and outputs)
- ▶ topological structure of the evaluated object, definition of the basic structure, elements and relations, including maintaining topology (this part is the critical infrastructure element system architecture review) if the critical infrastructure element is part of network structure, the evaluation is done separately,
- ▶ technological architecture of critical infrastructure element (the list of technologies that are in the critical infrastructure element used to secure its target function, support and protection, highlighting the which functions are for the element critical)
- ▶ production correlation and time-sensitivity – level of lacking production (electricity – immediately , oil due to the oil reserves in the pipelines – from hours to day; work activities of the ministry – a few days)
- ▶ number of employees.

Determination of the Resilience Attributes and Indicator Values

- ▶ The Risk value (parameter / coefficient) H_{RZ} – the potential impact of risk on the critical infrastructure functionality,
- ▶ The Correlation value (parameter / coefficient) K_{SO} – expressing dependence and links between the different areas of critical infrastructure,
- ▶ The Structural robustness (parameter / coefficient) K_{SR} – elements ability to withstand the effects of negative factors due its structure, system performance and characteristics of technology,
- ▶ The Security robustness (parameter / coefficient) K_{RO} – referring to the status and level of security measures ensuring the elimination of risk exposure,
- ▶ The preparedness value (parameter / coefficient) K_{PR} – ability to provide an element response to an exceptional event / incident and restore the critical infrastructure element required functions.

Calculation of Critical Infrastructure Element Resilience for Selected Risk

- ▶ Mathematical expression of critical infrastructure elements resilience in relation to the i-th risk:

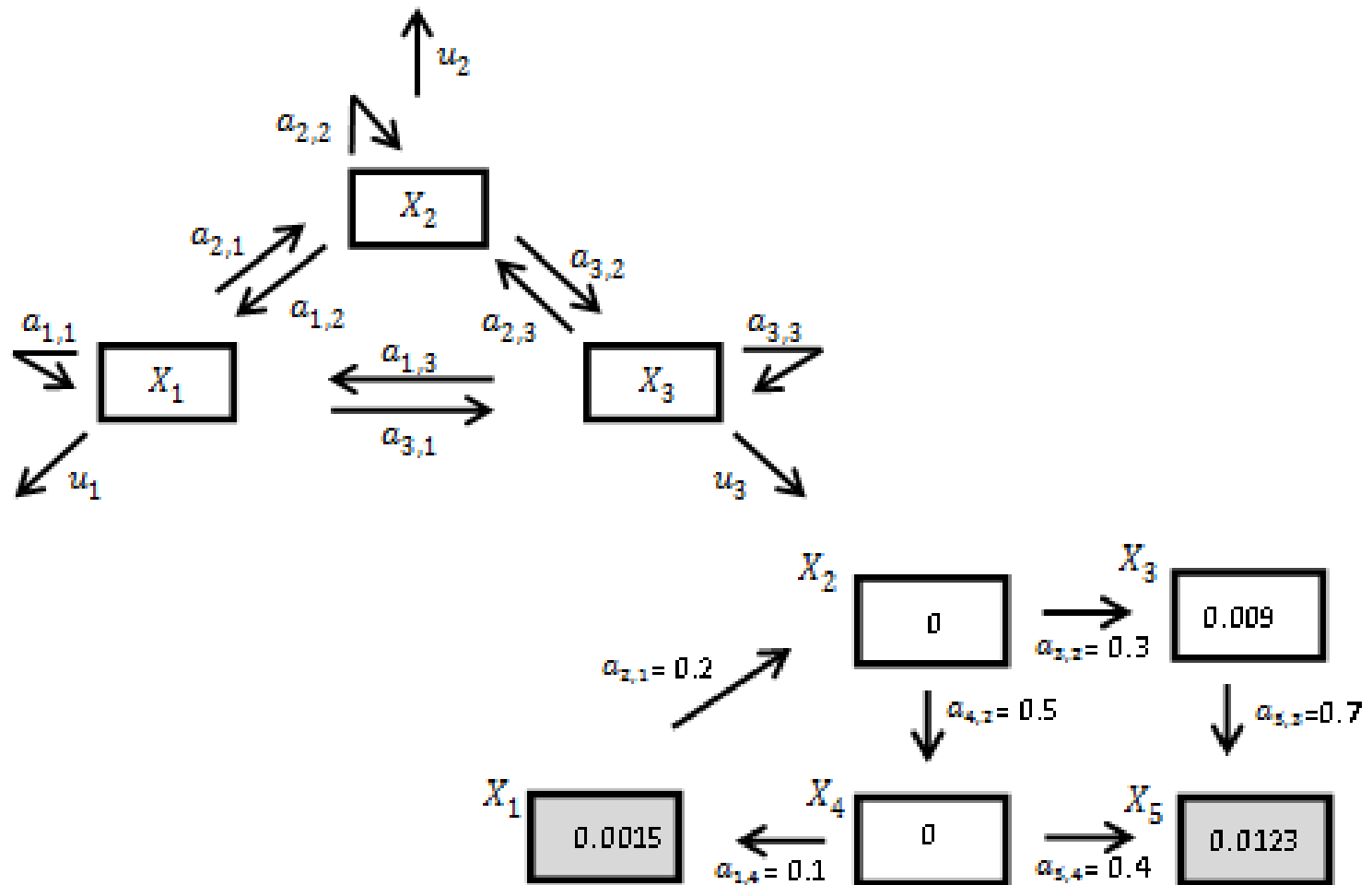
$$ODi = \frac{(1 - H_{Rzi}) + (1 - K_S) + (K_{RO} * V_{RO} + K_{PR} * V_{PR})}{3}$$

where:

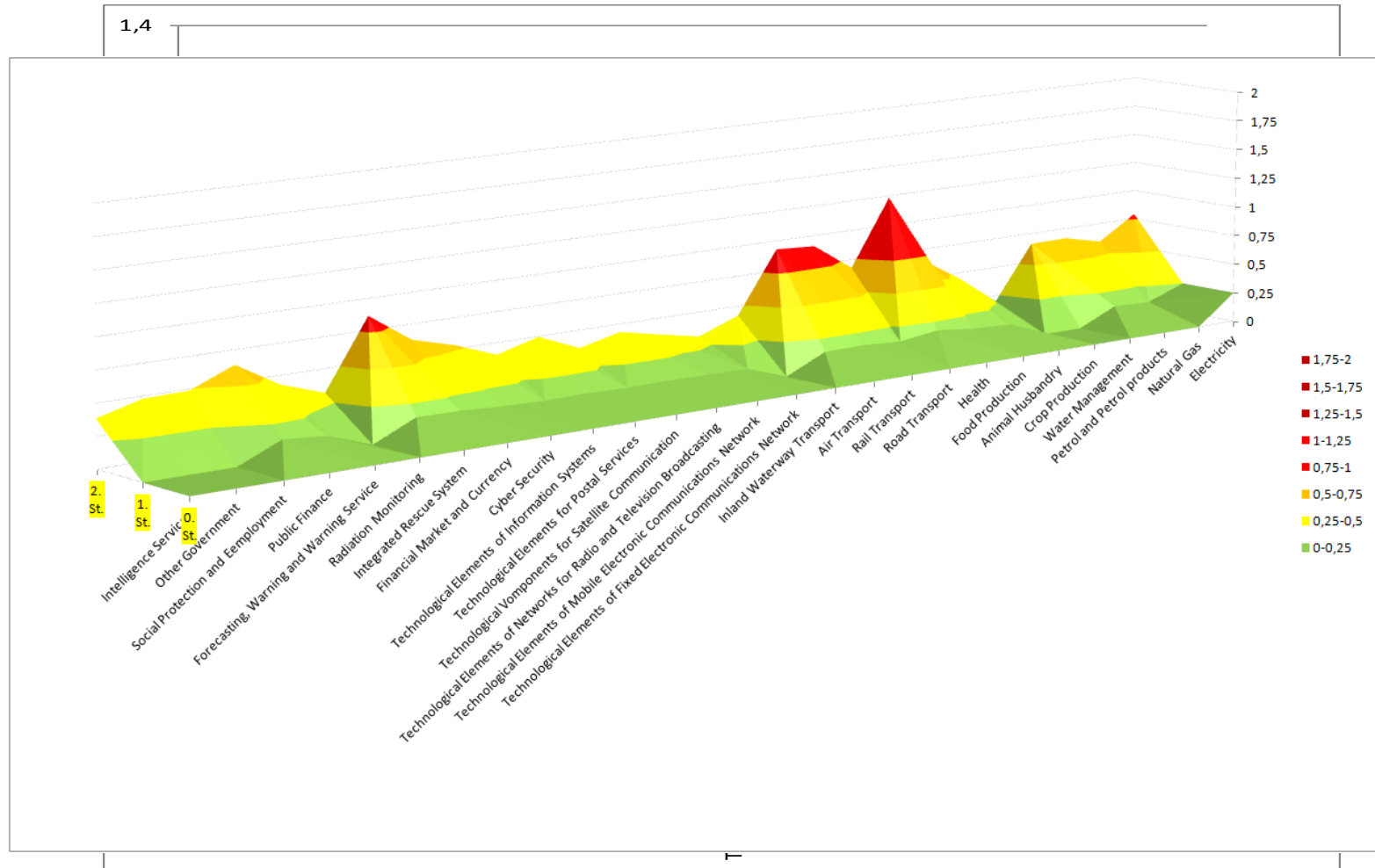
- ▶ H_{Rzi} – the value of i-th risk,
- ▶ K_S – correlation parameter,
- ▶ K_{RO} – robustness parameter,
- ▶ V_{RO} – robustness weight,
- ▶ K_{PR} – preparedness parameter,
- ▶ V_{PR} – preparedness weight,



Modelling of Domino and Synergy Effects – correlation parameter assessment



Modelling of Domino and Synergy Effects – correlation parameter assessment



Calculation of Critical Infrastructure Element Resilience for Selected Risk

- ▶ For a complex element or element

where:

- ▶ ODP – selected critical infrastructure element
- ▶ ODi – element resilience
- ▶ xi – number of critical infrastructure elements

	B	C	D	E	F	G	H	I
i	Risks	S	P	N	Hz	Hz	Odi	
Energetics								
1	Short-term electricity outage	2	0	0	X	X		
2	Long-term electricity outage	2	0	0	X	X		
3	Outage of water supply	1	0	0	0	0.00		
4	Outage of gas supply	1	3	2	0.24	0.73		
Natural impacts								
5	Flood	2	0	0	X	X		
6	Prolonged drought	4	0	0	X	X		
7	Extreme heat and drought	3	0	0	X	X		
8	Thick frost	2	0	0	X	X		
9	Pandemic, epidemic	4	0	0	X	X		
Risks associated with the human factor								
10	Conflagration	4	0	0	X	X		
11	Explosion	2	0	0	X	X		
12	Robbery	2	0	0	X	X		
13	Leaks of pollutants in the area	2	0	0	X	X		
14	Outage in logistics	2	0	0	X	X		
15	The virtual attack	3	0	0	X	X		
16	The terrorist attack	1	3	3	0.36	0.69		
17	Disruption of public order	4	0	0	X	X		
18	Unavailability of staff	2	0	0	X	X		
19	Sudden rush of patients	4	0	0	X	X		
20	Technical failures	2	0	0	X	X		
21	Sabotage	4	0	0	X	X		
22	Violent criminal activity	1	3	4	0.48	0.65		
23	Acts of vandalism	4	0	0	X	X		
24	Plundering	1	0	0	0	0.00		

ODP 0.41

critical infrastructure element resilience relationship:

value with risk



Final Critical Infrastructure Element Resilience Evaluation



This work was supported by the research project VI20152019049 "RESILIENCE 2015: Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems", supported by the Ministry of the Interior of the Czech Republic in the years 2015-2019.



Thank you for your attention!!!



Univerzita Tomáše Bati ve Zlíně