Risks in the energy system and a multivalued modal logic approach to identify adverse cyber events

Ionut PURICA

Prof.Dr.ing.Dr.ec.c.m.AOSR

Content

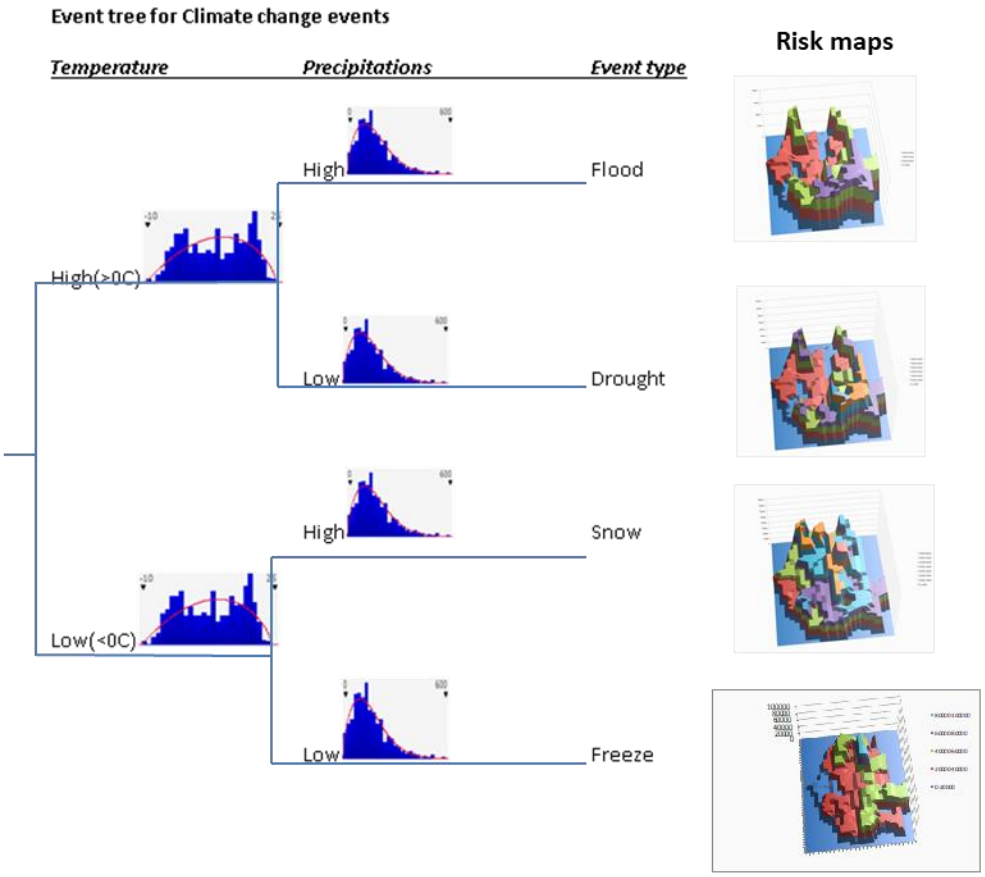
- Risks for the energy system
- Climate
- Potential cyber
- Volatilities
- Network
- Climate
- Models

Risks for the energy system

Several risks are presented that undermine the energy system and comments are made on the potential use of combined AI (artificial intelligence) and BI (biological intelligence) in mitigating and adapting to these risks.

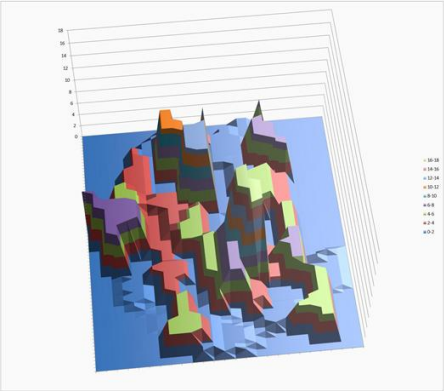
Climate

The climate risks are becoming more significant these last years due to the increase in the occurrence of climate change events. Looking at big data analysis on temperatures and precipitations in Romania's counties one may draw the climate change risk map of the country for various type of events: flood, drought, snow, and freezing, as shown below:

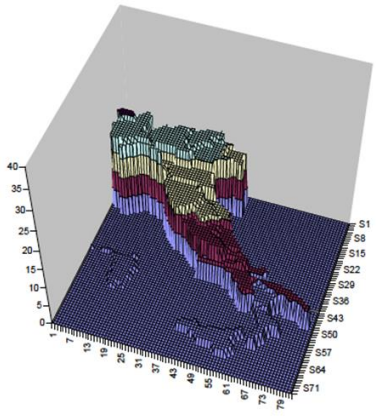


Moreover, there is a substantial impact on the critical infrastructures such as the gas network as shown below as a risk map and the power network as shown in pictures.

Romania gas grid CC and mechanical risk [probable deaths/1000 cap]



Natural gas risk in Italy [probable deaths / million inhabitants]



Critical infrastructure risk - hazards

Tower collapse (Shanghai)

Transformer after Earthquake (Chile)

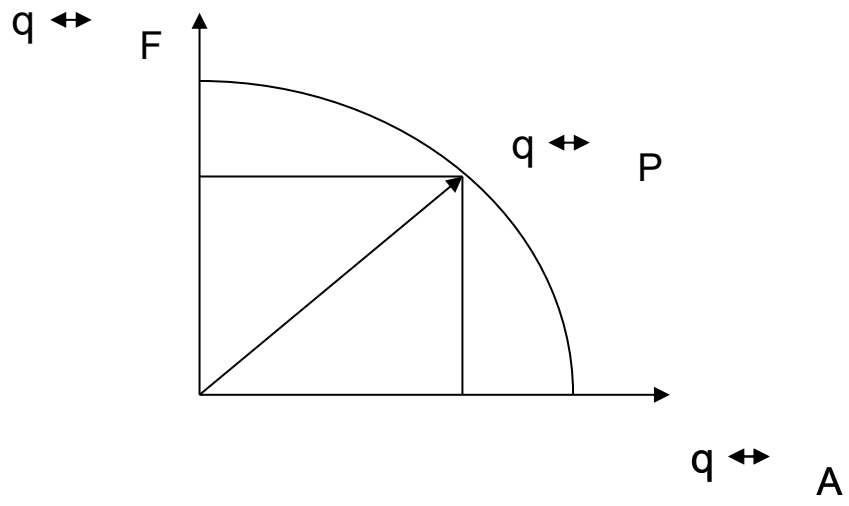
Station under flood (St.Louis, USA)

Terrorist attack (Colombia)

Source: IEEE Power & Energy nr.2, 2011

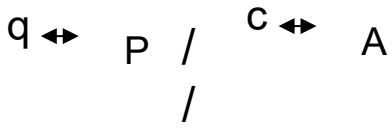
Cyber events

When looking at cyber related events one must try to prevent the occurrence of such events by accounting for the number of such events. To do this a nonbinary logic is more efficient in measuring the state of knowledge of the observer. Thus, the space of a logic values of possible events is defined where the truth and the false values are the usual ones in a binary logic. The formulae below describe the discernability of the observer in relation to the danger (truth) or lack of it (false) of a repeating cyber event.:



$$\mu^2_{q\leftrightarrow P} = \mu^2_{q\leftrightarrow A} + \mu^2_{q\leftrightarrow F}$$

Experiment



q – event

c – condition

Observation

$$n = n_A + n_F$$

Repeating condition c n times will rezult in situations with q true or false.

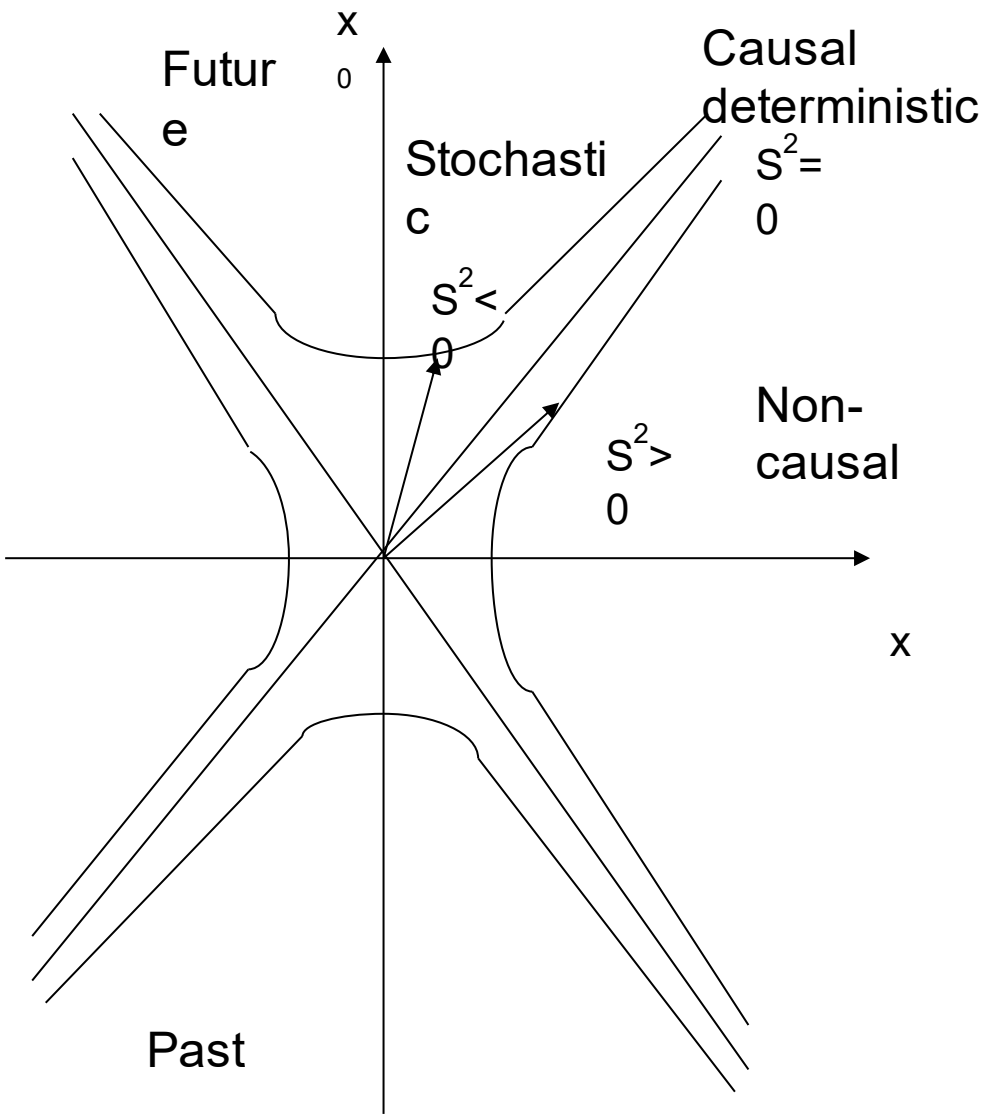
The state of knowledge of the observer and its the trajectory are resulting in the logic values space defined further on.

$$x_0^2 = n = \mu^2_{c \leftrightarrow A} \qquad x_1^2 = n_A = \mu^2_{q \leftrightarrow A}$$

$$x_2^2 = n_F = \mu^2_{q \leftrightarrow F}$$

$$S^2 = -x_0^2 + x_1^2 + x_2^2$$

$$S^2 = -x_0^2 + x^2$$ pseudo Euclidian bi-dimensional (Minkovski) space



The pass from a state of knowledge to another is described by a Lorentz transform in the Minkovski space. The evolution of the state of knowledge is associated with a ‘trajectory of knowledge’.

Conclusions on cyber events/attacks

The development of a new type of measure for the state of knowledge of the observer helps in determining the trend of various cyber events toward a state of risk leading to a possible attack.

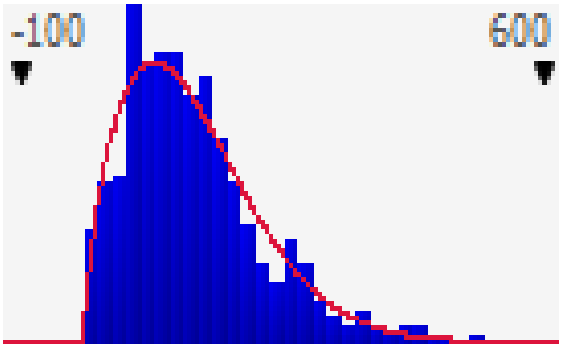
New threats need better protection methods.

Volatilities

Elements of security

According to the Security strategy of the energy systems launched by the EU Commission in 2014 it is necessary to have a diversified portfolio of electrical energy generation technologies that ensures the coverage of situations when various types of risks manifest themselves. The same applies for gas interconnectors and for the climate change risks impact on critical infrastructures. Cyber security adds to the above risks.

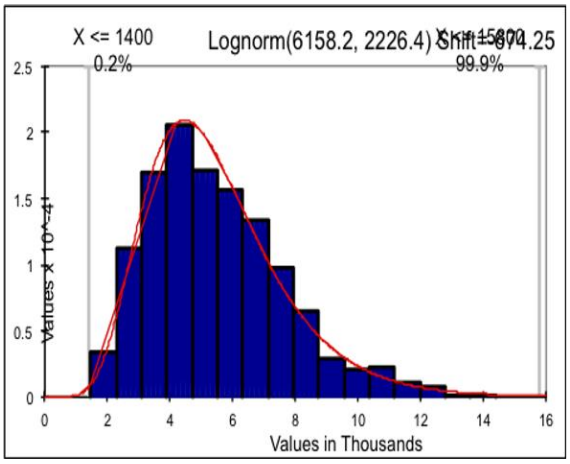
The advent of more hydro, wind and PV technologies in the last years have increased the volatility of the power system. An evaluation of the need for reserve power due to such volatilities is given for Romania as shown below.



Precipitations

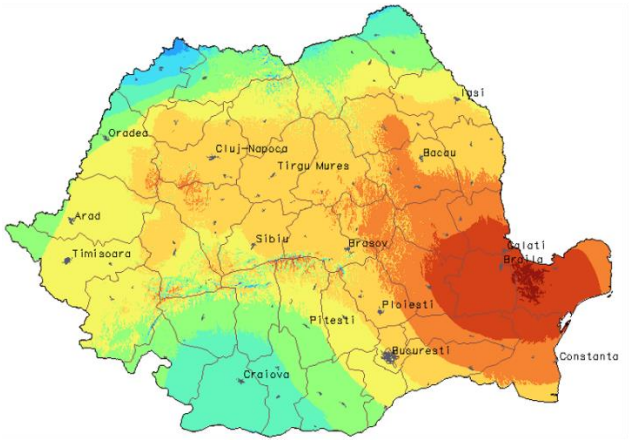
SD/Mean rain	0.65527311	hidro lake	
		TWh	16
		TWh lake	4.8
		h/year	8760
		exposure TWh	3.145310928
		power MW	359.0537589

Danube

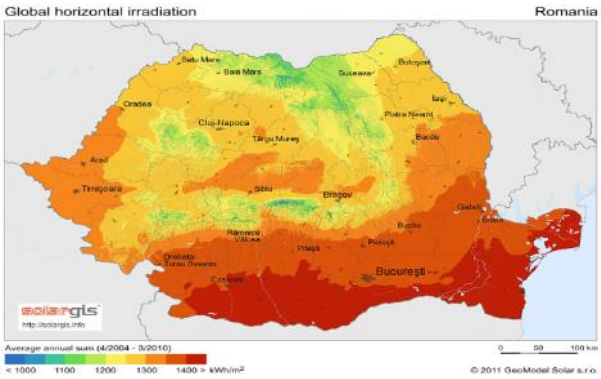


SD/Mean Danube	**0.361534215**			
		Needed security hydro run river		
		TWh	16	
		TWh run river	11.2	
		h/year	8760	
		exposure TWh	4.049183203	
		power MW	462.2355254	

Wind



SD/Mean wind	0.5	wind	
		TWh	3
		TWh wind	3
		h/year	8760
		exposure TWh	1.5
		power MW	171.2328767

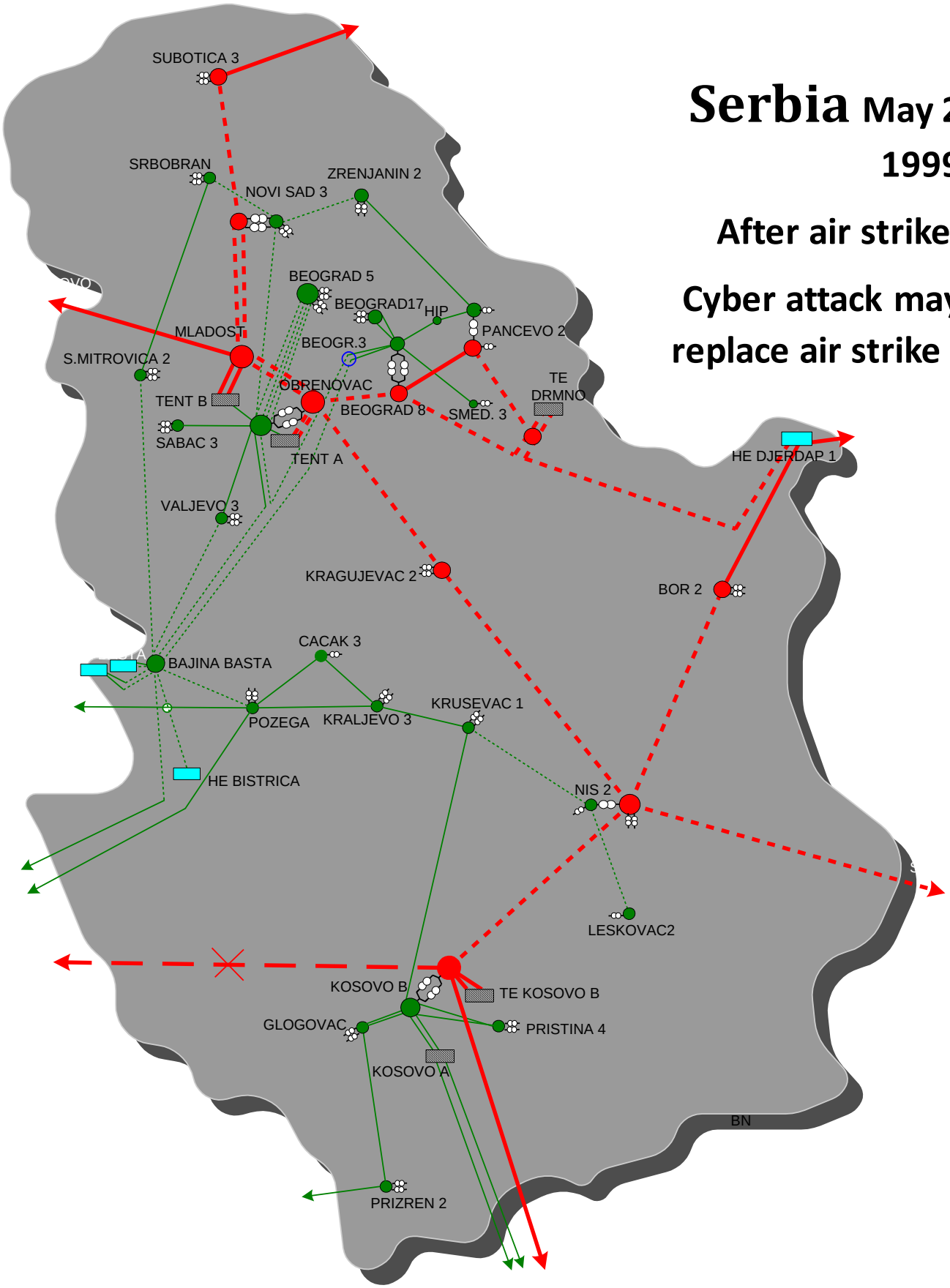


Photovoltaic

SD/Mean PV	0.6	PV	
		TWh	1
		TWh PV	1
		h/year	8760
		exposure TWh	0.6
		power MW	68.49315068

Networks

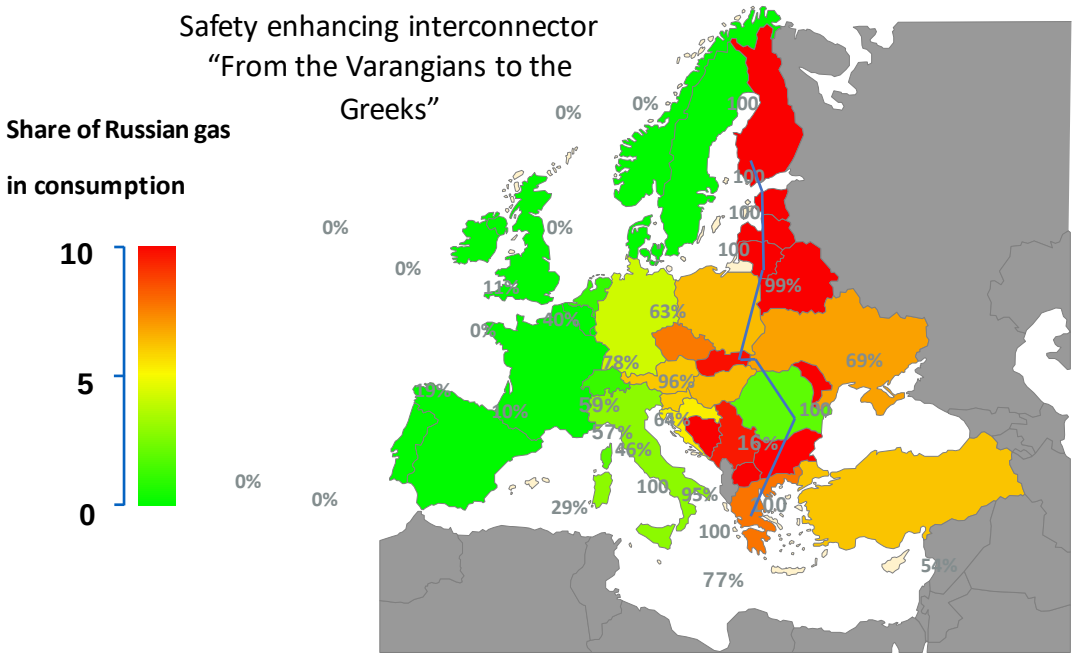
It is very important to secure the resilience of the power and gas networks. One example is the attack of the NATO on the Serbian power system in 1999 that identified 5 critical points to produce a total black out. A cyber attack may also produce the same effect by targeting the critical points of a given power grid. Moreover on a different view point the lack of an North-South interconnector of gas is seriously affecting the security of supply in East European Union. The two figures below are good examples of the above statements.



Serbia May 2 1999

After air strike.

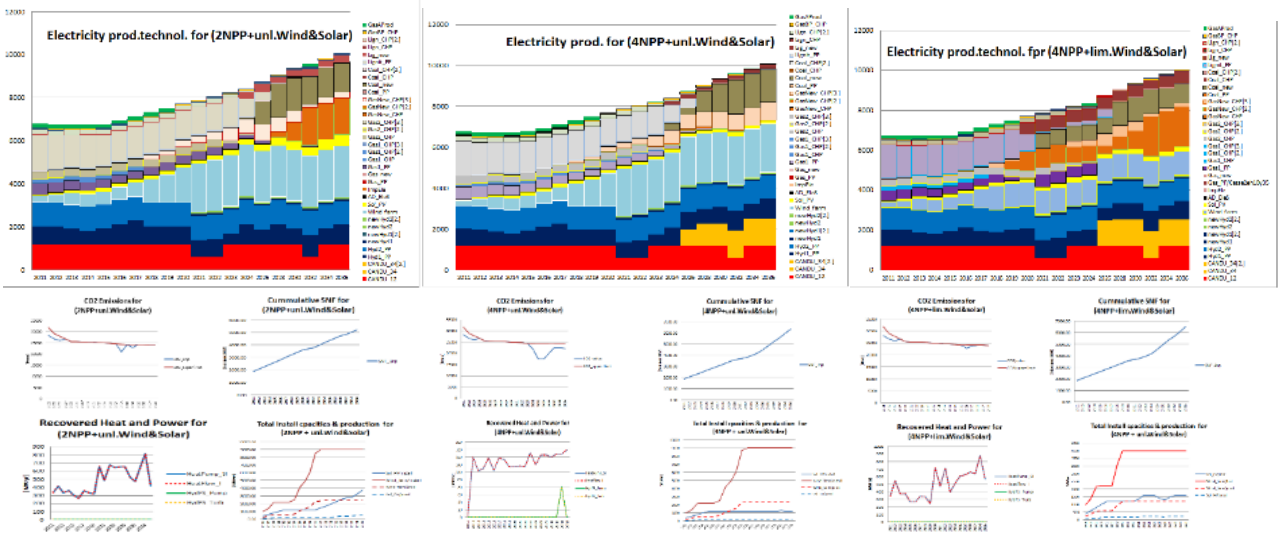
Cyber attack may replace air strike !



Source : CEDIGAZ- Estimate of international

Models

To better prepare for the future one needs to have the capability to analyse various scenarios such as to be prepared for emergencies. An example is given below on the result of applyind the MESSAGE model of IAEA to devise development scenarios for the Romanian power system.



Conclusions

The various elements of potential risks in the power systems have been presented with examples from several power systems.

It is important to note the need for combined implementation of both AI and BI – using advanced logic approaches adapted to the cooperation of the two systems – that increase the joint capability of both beyond the sum of their parts.

Also, an integrated view of the system must be considered for achieving the needed resilience of the system to various types of risk, ranging from the single facility to geostrategic scale of magnitude.

The above are only expressions of ideas that need a lot more analysis to be implemented at a geostrategic extension.