GLOBALIZATION OF POWER BUSINESS - THREAT OF BLACKOUTS?

Ivan Benes

CITYPLAN, Czech Republic[1]

Keywords

Critical infrastructure protection, blackout, public private partnership

Abstract

The Czech Republic has well developed national transmission grid. Nevertheless five emergency situations occurred this year (2006). The last one leaved about 2 millions people without electricity for several hours. The serious discussion between public and private sector, that has started already two years ago, was accelerated. Ministry of Interior, Ministry of Regional Development and three Regional Governments sponsored several studies and research projects how to improve population protection as well as critical infrastructure protection. We find out discrepancy between crisis legislation and energy ones.

Emergency situation according to crisis legislation activates measures to ensure emergency delivery of goods and services (for population protection). In the opposite, the emergency situation according to energy legislation activates measures to restrict or shut off the energy supply without penalty (for energy equipment protection). It creates gap between public responsibility (to ensure human safety) and private responsibility (to make profit).

Introduction

Human settlements have changed. Hundreds years ago the settlements were closed, self-sufficient and capable survive the siege. Today's cities are open and they can be hurt by attack on its infrastructure. We should understand well theirs resistance, dependency, complexity and vulnerability (Fig.1). City can be hurt by attack on its infrastructure.

[1] ivan.benes@cityplan.cz , http://www.cityplan.cz/ , ph.: ++420224922989, mobile: ++420603261470

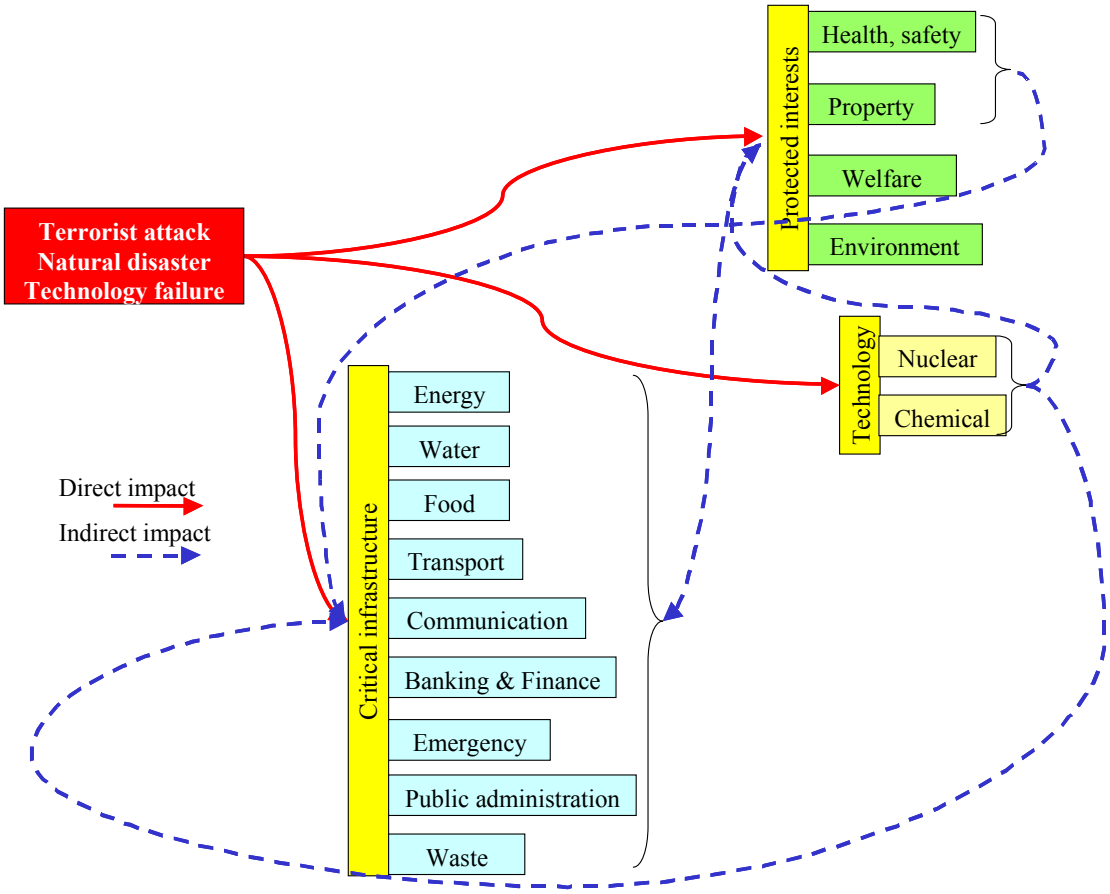

Fig. 1

Exposure to hazard comes from complexity and interdependency of critical infrastructure. Like a small fire can develop to firestorm in a similar way the trivial failure can develop to crisis situation through domino and cascade effect (Fig.2).

Protected interests can be hurt not only directly but also insidiously through critical infrastructure demotion (attack on the power grid, communication, water system, etc.). As well as attack against population can result into critical infrastructure demotion due to lack of personnel.

Problem arisen from globalization

Human safety is government's task. But once the infrastructures were privatized (energy, transportation, telecommunication, water supply, …) we can recognize the differences between private and public approach to the risk.

Whereas government takes care about sectoral and inter-sectoral availability, the private owner understands rather the project risk management, incident management plan and business continuity planning. It brings several problems. Private CI companies in the same sector are in the competitive position. Trouble of one company is a welcome opportunity for another. Therefore the sectoral cooperation is problematic. Private owner is shifting CI operation to their technical limits to be competitive enough. It can lead to lower safety, especially if supply interruption is free of penalty (i.e. exercise "force majeure" privilege).

Multiple terrorist attacks on critical infrastructure can cause crisis situation that exceeds capacity of rescue services. Significant hazard to human health and life as well as significant property loses can lead to activation of radicals and disintegration of democracy system (Fig.3).

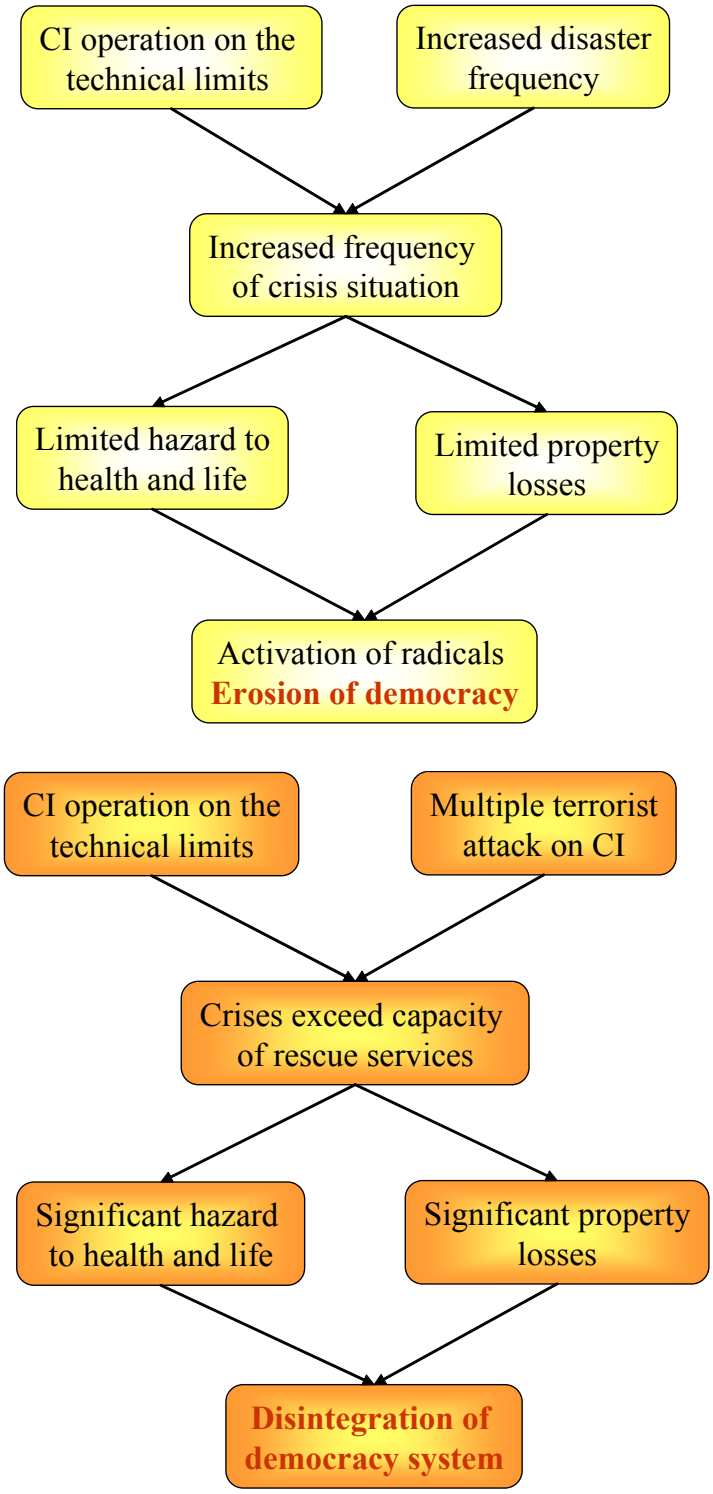

Fig. 2

Once in a while are some villages without electricity due the extreme weather conditions. Cost cutting leads to slim the faulty crews and so the local blackouts (longer then 24 hours) are more frequent. The 2 or 3 weeks blackout can result into chaos and it is jeopardy for democracy.

Conflict between safety management and market value oriented management is obviously seen in perception of emergency. Emergency status in crisis legislation is oriented on provision of necessary supply of goods and services on behalf of population protection. Emergency status in energy legislation is oriented on supply restriction or cut without penalty on behalf of energy facility protection. Bigger gap asks for higher capacity of Integrated Rescue Services (Fig.4). The gap can be overcome by legislation (symbolized by arrow).

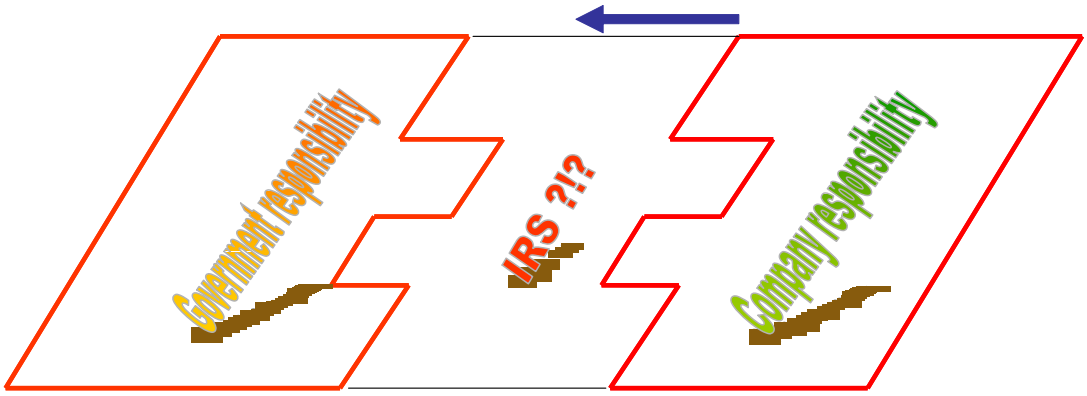

Fig. 3

Many energy infrastructure companies have well developed emergency response plans. Although these plans focus on responding to natural disaster and man-made errors, they still provide a solid basis for responding to the harms inflicted by a potential terrorist attack. However, far fewer companies have approached the issue of proactive security in a considered, comprehensive and proactive manner.

From the security point of view a strategic security plan should look at far more than fences, lights and guards. These plans should look at the broad range of business, public affairs, legal and regulatory issues that impact security, such as:

- How do we integrate our security planning into our business continuity planning?
- What informations are we providing publicly that we shouldn't and how do we change this? Why is this information being made public?
- What liabilities do we have and how can we limit them? What is our standard of due care in the wake of these attacks and are we meeting that standard?
- What legal and regulatory impediments are there to building redundancies and how can we overcome them?
- How do we communicate our security planning to stakeholders without compromising security in the process - both before a crisis and after?
- How do we plan on working with the authorities in handling these security issues - both before a crisis and after?
- How does the changing national security environment as a whole impact our business plans and models?

In an open democracy reliant upon a free market economy, security is necessarily imperfect. Further, in dealing with an industrial sector as extensive in scope and geography as the energy sector, it is impractical to suggest that this entire infrastructure could or should be rendered perfectly invulnerable to terrorist attacks.

Threat of blackouts

According to vulnerability analysis and risk scoring done in the project "Population protection and its dependency on energy critical infrastructure" (Institute of Population Protection, CITYPLAN, ViP, 2004-2005) the national grid (transmission system 400kV and 220 kV) is the most critical part of energy infrastructure (Fig.5). X-axis represents relative expression of the risk scoring.

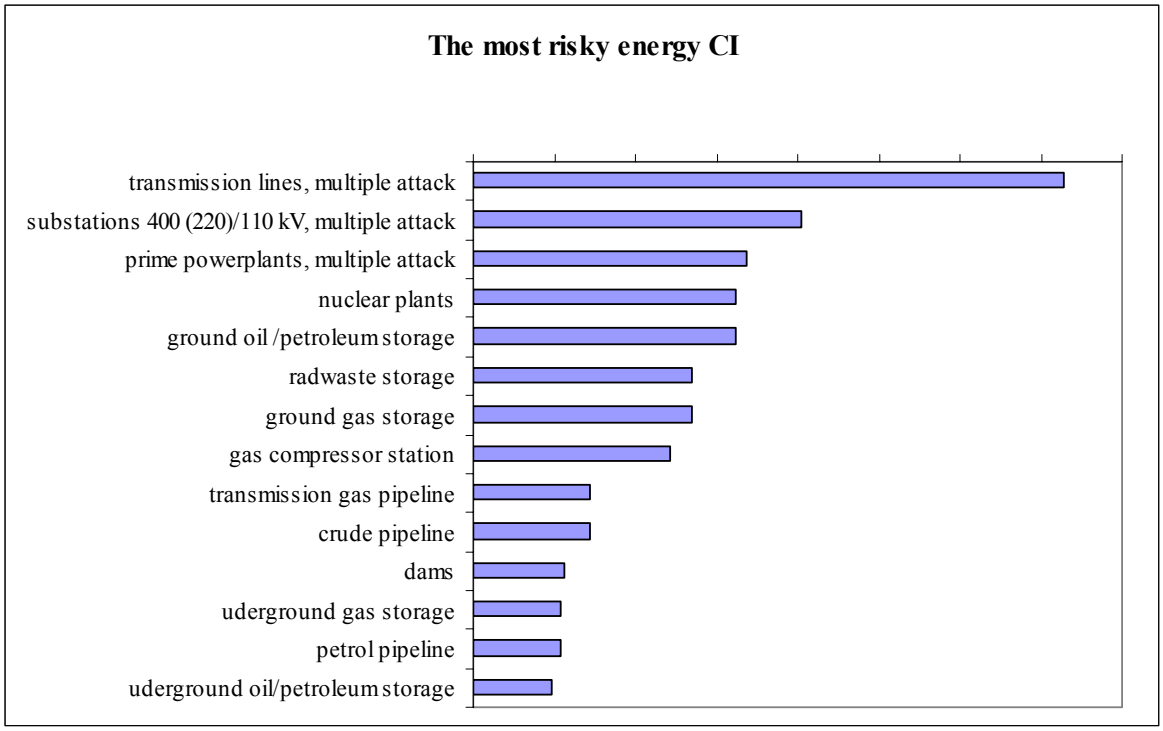

Fig. 4

After 9-11 attack in USA, as well as attacks in Madrid and London show, that N-1 rule is not sufficient enough to ensure protection against blackouts. On 14 August 2003 a large section of national grid failed leaving 50 million people in the US and Canada without power. And not just without power; in Cleveland pumping stations shut down leaving people without water; in Toronto subways were out of action for several days. Then it happened in Europe. In quick succession major power outages occurred in Southern Sweden and in Italy. It can happen also in the Czech Republic, because the Czech national grid operation is also under pressure of power traders.

Critical infrastructure should be equipped with the immune system. Time is the key factor that determines extent of losses. Our critical infrastructure structures are almost as ingenious as skeleton. Our critical infrastructure piping is almost as ingenious as bloodstream. Our critical infrastructure control systems are almost as ingenious as nervous system. But we are missing something what is ensured by lymphatic system. We need to be prepared not just for single event, but much more.

Immune system knows to treat hundreds attacks of viruses and bacilli a year and most of them is able eliminate automatically without our brain and without doctor. This is big challenge for research, development and innovation that should lead to self-healing critical infrastructure

systems. Public Private Partnership can facilitate this effort if the sustainable development will be based on the safety management and business continuity planning.

RESPO Project

Last year RESPO (RESilient Power) project has started. Project is granted by Czech Ministry of Trade and Industry. Project will solve the resilience of power distribution against the national grid blackout. About 38% power generation in the Czech Republic comes from power plants and district heating plants connected to the distribution grids. Because ancillary services are provided by the national grid, during power outage of national grid today's distribution grids are not able to balance local power generation and load.

RESPO project will solve the crisis demand side management that enables to regulate and provide necessary power to customer and critical infrastructure facilities. Project team is constituted from five research companies led by the CITYPLAN.

Project should contribute to enhance current European electricity networks to be sufficient to meet challenges and policy imperatives of the 21st century, especially from the human safety point of view. RESPO project is in the line of the SmartGrids European Technology Platform for Electricity Networks of the Future (Fig. 6).

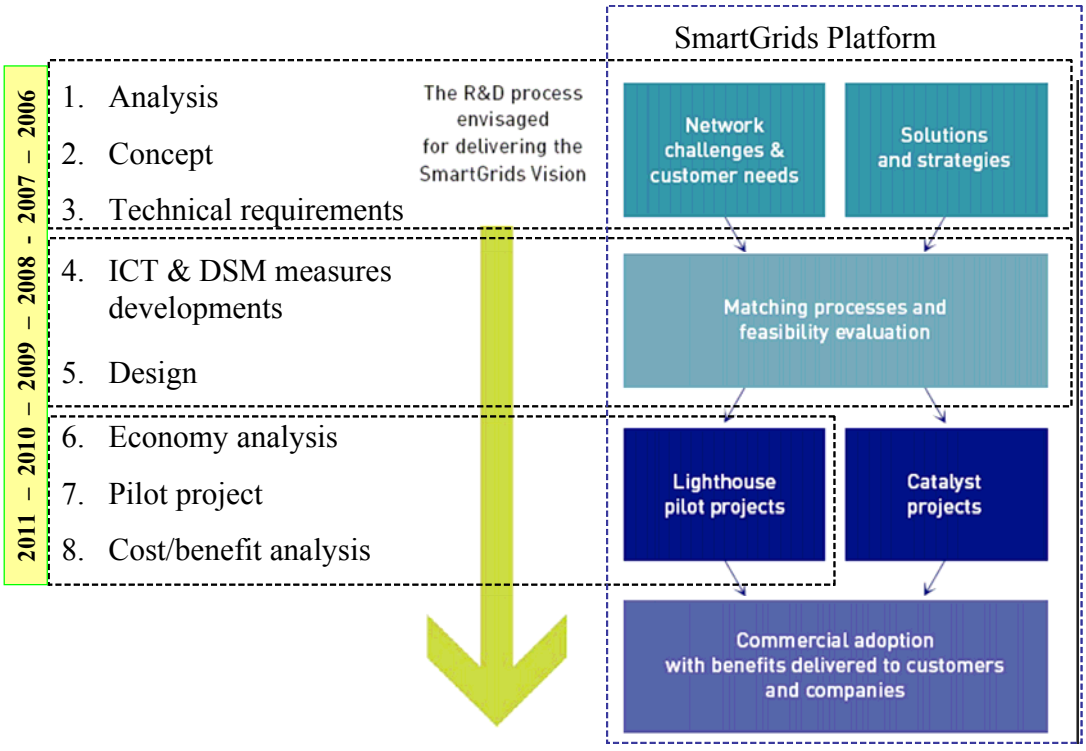

Fig. 5

The figures show, that RESPO project fits well the SmartGrids platform.

Results

Critical infrastructure protection is no imaginable without Public Private Partnership. In the Czech Republic this problem is solved on three levels (Fig.7).

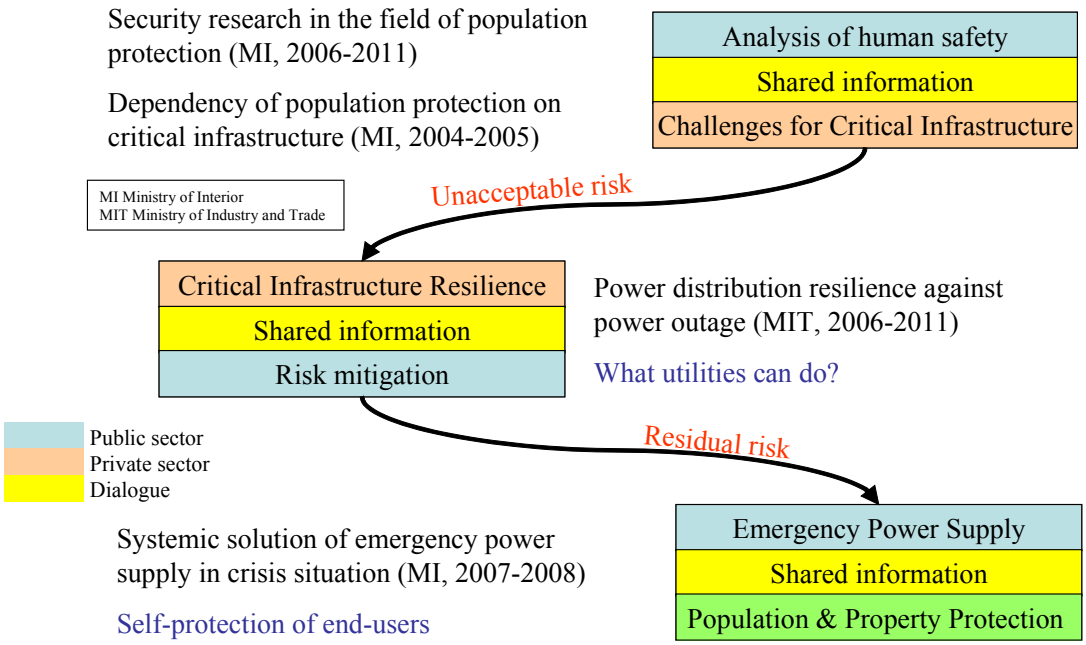

Fig. 6

On the national level the public sector provides analysis from the holistic view on the human safety. We provide vulnerability analysis, impact analysis and risk assessment. The results address the challenges towards private sector to mitigate unacceptable risk.

On the second level the owners and managers should look for measures to provide resilience, protection and defence of critical infrastructure facilities and technology. The good praxis to improve security and service continuity is the Business Continuity Management and Incident Management Planning.

The residual risk is then shifted on the end-users. If measures implemented by utilities will not be sufficient, the residual risk will be higher and it should be overcome by end-use measures. On this third level population should be advised to provide self-protection as well as the commercial sector should be advised to provide business continuity planning.

Discussion

It will be challenging task to the future to harmonise understanding of what a certain security level means (terms of level of protection, organisation, procedures, etc.) between different private, public and (inter)national bodies and different languages, and organisational and legal systems.

This requires also development of ontology to support effective communication between (inter)dependent critical infrastructures across national borders.

Author's Biography

Mr. Benes is general manager of CITYPLAN - engineering and research company. He has more than 35 years of experience in the engineering, economy and management. His areas of particular expertise include critical infrastructure protection, business continuity planning, energy engineering and economy analysis.