FACTORS OF VULNERABILITY AND RESILIENCE IN ENERGY SYSTEMS

Kari MÄKI
VTT – Finland
kari.maki@vtt.fi

Kim FORSSÉN
VTT – Finland
kim.forssen@vtt.fi

Minna RÄIKKÖNEN
VTT – Finland
minna.raikkonen@vtt.fi

ABSTRACT

This paper addresses factors of vulnerability and resilience for critical infrastructures (CIs). Such factors mean elements contributing to vulnerability, for instance structural weaknesses, low maintenance level or infrastructure age. On resilience side such elements include for instance improved condition monitoring, better preparedness planning or various technical solutions. The analysis conducted considers these factors on a generic level for all critical infrastructures and after that focuses on energy systems and their specific characteristics.

The information obtained for vulnerability and resilience factors is highly useful for CI operation and policy purposes. At the same, the methodology developed can be applied for different data sets or can be developed further for more detailed analysis.

INTRODUCTION

This report focuses on analysis of factors contributing to CI vulnerability and resilience. To obtain this, the work performed utilizes MOVE conceptual framework [1] for identifying dimensions of vulnerability. MOVE framework defines six dimensions of vulnerability: Physical, Ecological, Social, Economic, Cultural and Institutional dimension. This methodological framework serves for CI vulnerability assessment and analysis of CI protection measures.

This work is conducted within EU FP7 project INTACT [2] (Impact of Extreme Weather on Critical Infrastructures) in close co-operation with project's country cases. Stakeholder interviews have been conducted via cases organization in following countries: Finland, Ireland, Italy, Spain and Netherlands. In addition stakeholder interviews have taken place for instance in Germany and Norway.

OBJECTIVES

The objective of this work is to support CI operators and policy makers in understanding CI vulnerabilities with relation to extreme weather events and to provide information on potential measures for reducing such functionalities. Characterization of factors behind vulnerability and resilience provide essential information for these purposes.

STAKEHOLDER INTERVIEWS

In INTACT, there are five case studies defined as presented in Table 1. Together they cover the most important extreme weather events in a variety of regions in Europe.

Table 1. INTACT case studies and their characteristics.

Case Study	*Country*	*Hazard*	*CI considered*
A	Ireland	Storms, heavy rain, flash floods	Urban CI
B	Netherlands	Storm, flooding, rainfall,	Transport (roads, railroads, pipelines)
C	Italy	Rainfall, Landslides	Transport
D	Finland	Snow storm	Electric power supply
E	Spain	Heat waves, droughts	Networked infrastructure,

Each case study has taken part in this work by means of conducting stakeholder interviews. During this work, total of 58 templates for identifying factors for vulnerability and resilience have been completed. In addition to INTACT case studies, information has been collected from other relevant stakeholders and project partners. Key statistics for the templates are presented in Table 2.

Table 2. Statistics on CI sectors covered by stakeholders interviewed.

Interviews in total	*58*
Energy	12
Transportation	29
Water management	5
Emergency services / government	6
IT and communications	2
Food production	4

These interview templates mention altogether 176 factors of vulnerability and 179 factors of resilience. These factors have been categorized for further analysis. Both the frequency with which they are mentioned in the templates and their level of importance have been used to estimate their significance factor. Based on this, most important factors for different case sets can be presented.

The importance has been questioned as a respondent opinion with a scale (Very Low…Very High), which has been transferred in to numerical values 1…5. At the same, vulnerability dimension has been questioned.

GENERIC RESULT ANALYSIS

Vulnerability factor analysis

For all data available, the vulnerability factor categorization based on questionnaire answer sets is presented in Table 3. Here the categorization has been made by grouping the interview responses. The categories thereby follow the issues mentioned.

Table 1. Top 5 vulnerability factors across all CIs.

Vulnerability factors TOP 5	*N*	*AVERAGE*	*%*	*IMPACT FACTOR*
Infrastructure age, weakness, maintenance level	29	4,31	50,00 %	**2,16**
CI location or structure related	25	4,56	43,10 %	**1,97**
Nature-related; severity of EWE	23	4,61	39,66 %	**1,83**
Cross-infra impacts (cascading, deteriorating)	22	4,55	37,93 %	**1,72**
Special circumstances (area, soil, temperature, etc.)	19	3,89	32,76 %	**1,28**

The observations show that main vulnerabilities are seen in issues relating to infrastructure condition. Typically this relates to component ages, too weak-built structures but also to inadequate maintenance levels. Another common factor is the location of CI and the system structures, which are based on earlier planning and are now difficult and expensive to modify. Severity of EWE is mentioned as one important factor, which is obvious, however not very informative aspect in this study.

Additionally, vulnerability factors were compared between CIs represented in the questionnaires. The main observations have been illustrated in Figures 1 and 2.

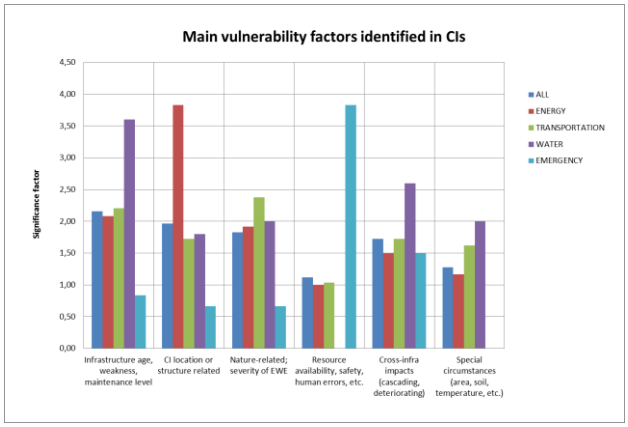

Figure 1. Main vulnerability factors across CIs.

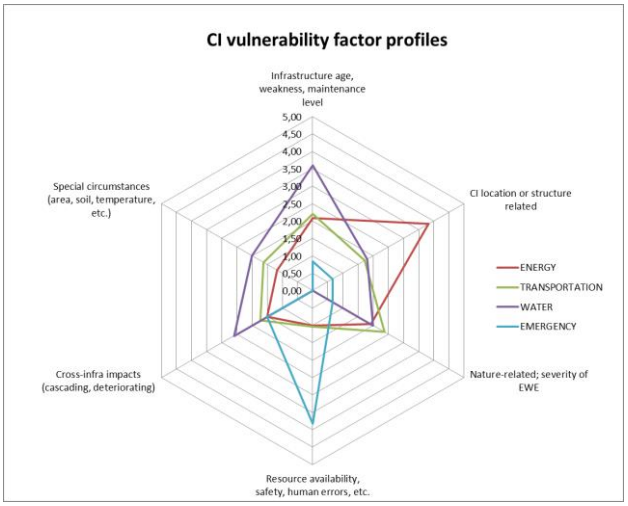

Figure 2. CI vulnerability factor profiles.

These results reveal some obvious differences. For instance on water sector infrastructure condition seems to be the main concern, whereas energy sector is struggling with the location and design of their existing infrastructure in contrast to extreme weather events. Emergency services consider the resource related aspects crucial but are not specifically concerned about technical aspects.

Resilience factor analysis

Similarly to vulnerability factors, project questionnaire also covered resilience factors. Factors were gathered and mapped in terms of their implementation stage, disaster cycle stage, importance and vulnerability factor they contribute to. Similar to vulnerability factors, these factors were categorized and analyzed.

Table 4. Top 5 resilience factors across all CIs.

Resilience factors TOP5	*N*	*AVERAGE*	*%*	*IMPACT FACTOR*
Technical solutions	36	4,58	62,07 %	**2,84**
Improved maintenance, inspections, condition monitoring	31	4,74	53,45 %	**2,53**
Improved preparedness planning	20	4,90	34,48 %	**1,69**
Adjusting operation principles and processes	18	4,44	31,03 %	**1,38**
Communication, warning systems	16	4,75	27,59 %	**1,31**

The observations show that resilience factors gathered in this work relate mainly to practical solutions and risk management actions that CI operators undertake.

Technical solutions are applied widely and improved condition monitoring is also mentioned commonly. Improving preparedness planning or communications are also rather high on the list.

Additionally, main resilience factors were compared between CIs represented in the questionnaires. The main observations have been illustrated in **Error! Reference source not found.**.

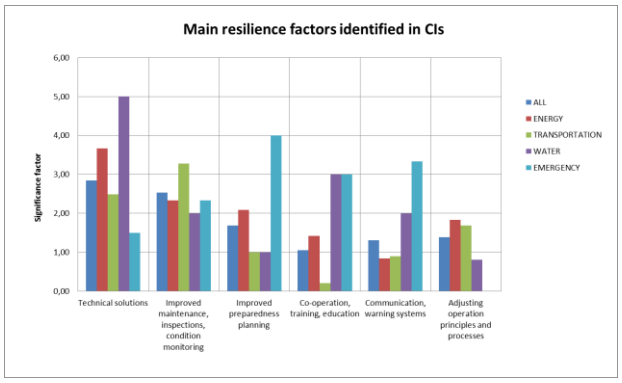

Figure 3. Main resilience factors across CIs.

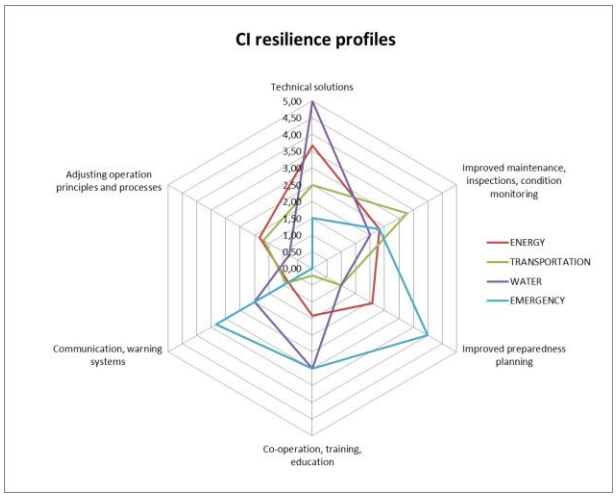

Figure 4. CI resilience factor profiles.

Some observations can be made on these results. Infrastructures such as electricity or water rely heavily on technical solutions for overcoming the extreme weather impacts. On the other hand, transportation sector is more relying on maintenance and condition monitoring methods. Emergency service providers are mostly looking at communication and warning systems, actor co-operation as well as improving preparedness planning. These conclusions seem very realistic.

It is also interesting to look at the bias of each profile. Transportation is clearly biased on technical aspects only, whereas emergency services are biased on planning and information exchange aspects. Energy and water show somewhat balanced share on all areas of resilience.

ENERGY SECTOR SPECIFIC ANALYSIS

The data has been further analyzed on each CI sector level. As a part of this, the factors for vulnerability and resilience are mapped against each other in order to see the completeness of available risk management actions. Here a special attention is on energy sector, especially electricity networks.

Tables 5 and 6 summarize the most important vulnerability and resilience factors for energy sector.

Table 5. Top 5 vulnerability factors for energy sector.

Vulnerability factors TOP 5	*N*	*AVERAGE*	*%*	*IMPACT FACTOR*
CI location or structure related	10	4,60	83,33 %	**3,83**
Infrastructure age, weakness, maintenance level	5	5,00	41,67 %	**2,08**
Nature-related; severity of EWE	5	4,60	41,67 %	**1,92**
Difficult to forecast, follow, monitor	5	4,20	41,67 %	**1,75**
Cross-infra impacts (cascading, deteriorating)	4	4,50	33,33 %	**1,50**

Table 6. Top 5 resilience factors for energy sector.

Resilience factors TOP5	*N*	*AVERAGE*	*%*	*IMPACT FACTOR*
Technical solutions	10	4,40	83,33 %	**3,67**
Improved maintenance, inspections, condition monitoring	6	4,67	50,00 %	**2,33**
Improved preparedness planning	5	5,00	41,67 %	**2,08**
Adjusting operation principles and processes	5	4,40	41,67 %	**1,83**
Affecting prevailing circumstances through planning or operations	5	4,40	41,67 %	**1,83**

Based on the observations, energy sector is highly dependent on the existing locations and structures of current infrastructure. Long planning and write-off periods and related slow renewal of infrastructure can be seen in the answers. Asset management methodology is well advanced in many cases; relating efficiency optimization can result in inadequate preparedness against extreme weather events. Aging infrastructure is commonly seen as

a vulnerability factor. On energy sector, regulatory framework commonly defines the reliability requirements applied also during extreme weather events. Interestingly regulation and incentives do not gain any major attention in this questionnaire. Another common development is increasing outsourcing of field crew operations. This does not result in concerns relating to resource availability or lack of competence.

The resilience options rely strongly on technical solutions. Increasing underground cabling is mentioned as one solution against extreme weather events. At the same, applying different smart grid technologies is proposed as an option or as an addition to cabling. Improved maintenance and especially condition-based maintenance is commonly mentioned as a means of improved resilience. Preparedness planning is also mentioned, referring mainly to improving response during events through better preparation. However, co-operation with other actors is not identified as significant resilience factor here.

The vulnerability dimensions focus on physical aspects but include also quite balanced set of ecological, economic, social and institutional dimensions. Generally, questionnaires among energy sector operators show rather good awareness and commitment on other infrastructures and cascading impacts energy system can result in. On the other hand, as stated above co-operation is not seen as a major aspect.

Compatibility of major vulnerabilities and resilience actions were also compared as a part of this analysis. These aspects are mapped against each other based on the information gathered within the questionnaire. Figure 5 illustrates the outcome in the form of gap profile.

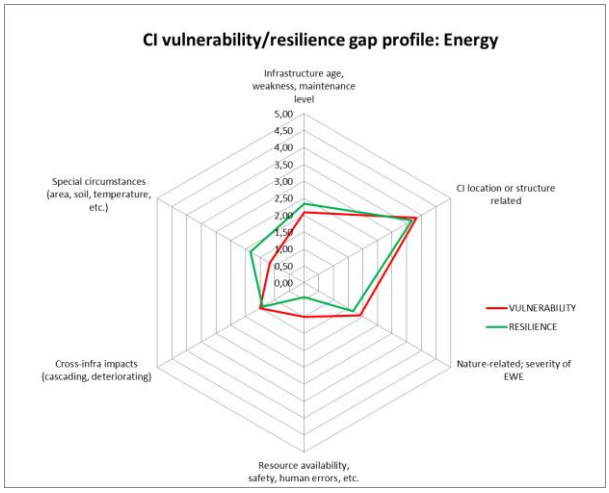

Figure 5. Energy sector vulnerability/gap profile.

Energy sector seems to be well aligned with vulnerabilities and means for overcoming them. Regarding for instance CI structures, age, maintenance aspects or extreme weather event forecasting, necessary actions seem to be well balanced. However such actions are commonly considered to be expensive for wide-scale utilization. Some minor gap can be seen in resource availability and crew operations – vulnerabilities identified are not fully met with suitable resilience actions.

CONCLUSIONS

In this work the MOVE framework has been applied for categorizing vulnerability factors. Similarly, disaster cycle model has been utilized in dimensioning the resilience actions. Such frameworks seem applicable for various data sources applied during the work.

The results show that it is possible to differentiate vulnerability and resilience factors for different CIs. Further this data can offer some information on gaps between vulnerability and resilience. By expanding the data available for analysis, the results could be made even more reliable.

The work reported here has focused on factors of critical infrastructure vulnerability and resilience. The main development in this work has been wide collection of data from European stakeholders by means of questionnaire. This questionnaire was in total answered by 58 stakeholders who identified 176 vulnerability factors and 179 resilience factors. This data has been processed in order to find important characteristics and to be able to evaluate different infrastructure sectors in comparative means.

Generally, the results indicate that actions taken or planned currently match the technological vulnerabilities such as infrastructure aging or design fairly well. At the same, the results indicate that most immense gaps are found in cross-infra impacts, resource-related aspects and forecasting/monitoring severity of external events.

REFERENCES

[1] Vinchon et al, 2011. Assessing vulnerability to natural hazards in Europe: From Principles to Practice: MOVE Project.

[2] Michael McCord, John Rodgers, Peadar Davis, Martin Haran, Claudia Berchtold (2015): SOTA gaps and guidance parameters for all WP's, INTACT Deliverable D1.1, project co-funded by the European Commission under the 7th Framework Programme.