Risk and Vulnerability Analysis of Critical Infrastructures - The DECRIS Approach

I. B. Utne[a], P. Hokstad[b], G. Kjølle[c], J. Vatn[a], I. A. Tøndel[d], D. Bertelsen[e], H. Fridheim[f], J. Røstum[g]

[a] *Norwegian University of Science and Technology (NTNU), Department of Production and Quality Engineering, Corresponding author: Ingrid.b.utne@ntnu.no*
[b] *SINTEF Technology and Society, Safety and Reliability, Trondheim, Norway*
[c] *SINTEF Energy Research, Energy Systems, Trondheim, Norway*
[d] *SINTEF ICT, Software engineering, Safety and Security, Trondheim, Norway*
[e] *SINTEF Technology and Society, Road and Transport Studies, Trondheim, Norway*
[f] *Norwegian Defense Research Establishment, Kjeller, Norway*
[g] *SINTEF Building and Infrastructure, Water and Environment, Trondheim, Norway*

Abstract
A Risk and Vulnerability Analysis (RVA) method for critical infrastructures is being developed in the SAMRISK project DECRIS (Risk and Decision Systems for Critical Infrastructures). The method supports an "all hazards" approach across sectors; i.e., electricity supply, water supply, transport (road/rail), and information and communication systems (ICT). The main focus is on serious events, and the DECRIS approach is an enhanced RVA, focusing on serious events and emphasizing dependencies between the sectors. The end users of the method and decision support systems are local governments, municipalities, and companies responsible for the infrastructures. The objective of this paper is to present main features of the method and discuss some preliminary findings from the project's case study of Oslo municipality.

Keywords: Critical infrastructure; Risk and vulnerability analysis; Societal security and safety

1.0 Introduction

Probabilistic Safety Analysis (PSA) and Quantitative Risk Analysis (QRA) have been applied for decades as an integral part of the safety management in nuclear power plants and other industrial process industries. PSAs and QRAs comprise detailed probabilistic models like fault- and event trees, and physical models of, e.g., fire and explosion development. In Norway, it was recognized that these type of risk models require more knowledge and resources than available in small and medium enterprises and in the public sector. Therefore, in the early nineties, a much simpler approach was developed under the acronym ROS. In this presentation we will use the corresponding English acronym RVA (Risk and Vulnerability Analysis) to describe this methodology and our proposed extensions. The Directorate for Civil Protection and Emergency Planning (DSB) has the overall responsibility in Norway for coordination and ensuring that RVA are used in the management of critical infrastructures.

Today, the term "critical infrastructures" has become central in the emergency preparedness work of many nations, but there is yet no universally accepted definition of the term. Most definitions point toward systems that are of vital importance to the society (Rinaldi et al., 2001). Use of the term is often related to (inter)national security challenges and exemplified by technological networks like energy supply, transport services, water supply or information and communication services (Doorman et al., 2006; Røstum et al., 2008). Failures of these systems can cause major damage to the population, the economy or the national security: Hence the need to identify relevant safety/security measures, hence the need for risk analysis.

The current format of an RVA is very similar to a preliminary hazard analysis (PHA) where the starting point is the identification of undesired events, followed by a simple probability and consequence assessment of each event. Even though the simplicity of the analysis is appealing, the current RVA faces several methodological challenges, such as:

- Complexity: Critical infrastructures are complex combinations of old and new technologies, involving behavioral issues, economic considerations, and varying organizational and regulatory practices. How can we predict the outcomes of undesired events in such complex systems?
- Interdependencies: Failure in any critical infrastructure is likely to impact most other parts of society, including other critical infrastructures. How should we address these interdependencies in evaluating the consequences of incidents?
- Unified approach across sectors: There is a need for establishing holistic risk assessment frameworks across the infrastructures to support cross-sector priorities.
- Risk perception: The perception of risks will vary between stakeholders, and so the willingness to pay (WPA) to prevent and the willingness to accept (WPA) specific undesired incidents will vary between the analysts, the decision makers, and the public opinion. How will the different stakeholders influence the analysis results, and how should we best communicate the results of a risk analysis to different stakeholders?
- Lack of statistical data: We often lack data for many relevant incidents in the critical infrastructures.
- Development speed: The rate of change is fast in critical infrastructures. Any risk analysis will have a limited lifespan before it needs to be updated, so it is hard to ensure that proposed measures based on the analysis are still valid.

In Norway, RVAs have been applied and adapted for each sector independently, resulting in differences in the approaches. The DECRIS project utilizes experience from risk analyses within different critical infrastructures, and one of the main objectives is to develop an all-hazard generic RVA methodology suitable for cross-sector infrastructure analysis. Both safety (accidents, technological failures etc.) and security (malicious attacks) aspects shall be included. Further, the project will analyze issues regarding how the media and the public affect the decision process, and consider how different opinions may be combined to get a more appropriate system for decision-making across sectors.

The objective of this paper is to describe the preliminary risk analysis carried out in DECRIS in cooperation with the City of Oslo. First, we briefly describe the critical infrastructures involved, which are followed by an outline of the general RVA process in DECRIS. Finally, some preliminary results from the risk analysis in Oslo are given.

2.0 Critical infrastructures

DECRIS involves the critical infrastructures; electricity supply, water supply, transportation, and ICT. The following section gives a short overview of these sectors.

2.1 Electricity power supply

The electric power system consists of power production plants, transformers and grids transporting the electricity to the end-users. The grids consist of overhead lines, underground and submarine cables, divided into three levels: the central grid (transmission, the “highway”), the regional grid linking the transmission grid and the local distribution grids. There are interconnecting lines and

cables between neighbouring countries as well. Grid management and operation have been defined as a natural monopoly, where the users are tied to their local distribution company.

RVA for the power system (according to the regulations) is typically performed in qualitative terms based on expert evaluations, fault statistics etc. In quantitative risk assessment a major challenge is to identify chains of events that could lead to wide-area interruptions of the electricity supply. It is necessary to assess the propagation of power system component outages and to determine and evaluate the consequences of these cascading outages for the delivery points and end-users. For this purpose the methodologies of power system security and reliability analysis (e.g., (IEEE/CIGRE, 2004; IEC, 1999)) are important tools. The consequences for the electricity supply to the delivery points are typically described by indicators, such as number and duration of interruptions, and interrupted power and energy not supplied.

Over the last 10 – 20 years, there have been limited investments in new power plants and transmission lines, resulting in a strained power balance and increased utilization of the grids. The power system is an ageing infrastructure and the need for reinvestments is expected to increase rapidly the coming years. At the same time, the climatic changes may impose increased stress (more wind, icing) on the grids and there are some critical ICT dependencies in the system.

2.2 Water supply

The water supply system includes catchment area, source, water treatment system, and transport systems. Norway has a total of 46 000 km water mains. The largest owners are municipalities. Some smaller waterworks are privately owned, and some waterworks are intermunicipal companies. In total, there are 1600 waterworks delivering water to more than 50 persons each.

Several laws and regulations rule the service quality of the water supply system, and at present at least nine Ministries are involved, making it difficult for municipalities to keep updated on all regulations. The Norwegian Official Report (Government appointed commission, 2006) recommends that all regulations related to the water supply system becomes organized in one new sector law.

The waterworks owned by municipalities are non-profit businesses, and local politicians decide on strategies, operation plans, and fees. Currently, one of the major challenges with the water supply system is ageing. Also climate changes affect the system through, e.g., altered water quality, new pathogens, and extreme precipitation.

2.3 Transportation

The transport system consists of various transport networks and modes of conveyance for people and goods. In Norway today there are four main transport networks: Road, rail, air, and sea transport networks. Each of these networks comprises elements as junctions, bridges, tunnels, pavements and terminals with a lot of equipment, such as lighting, sign, and communication systems. Public authorities are responsible for the management of the Norwegian transport networks, however, management of roads, airports, and harbours are partly financed by user toll.

The means of conveyance include vehicles, such as cars and trucks, trains, trams, ferries, ships, and aeroplanes. Today, private companies take care of both scheduled and unscheduled transport services. In addition, leisure boats, private cars, bicycles, and walking count for a considerable number of everyday trips. Furthermore, there exists a considerable service industry for the transport

sector, including production and distribution of vehicles, fuel, and so on.

Norwegians make 3-4 daily trips with an average length of 5-10 km, 70-80 minutes a day are spent on travelling. 240 mill tons of goods are moved about 90 km every year, mainly by truck or ship. These transport activities imply some risk and result in about 350 fatalities every year; 300 of these on roads. Accidents are a major concern within all parts of the transport sector. A great number of RVAs and accident analyses have been carried out in a long period of time within the transport sector. Risks related to tunnel fire, transport of dangerous goods, and climate change are among the most focused issues for the moment.

Most of the transport activity is highly dependent on steady and sufficient energy and fuel supply, and on reasonable weather conditions. If not, people and goods will fail to reach their destinations, which accordingly may create severe problems for the performance of vital societal functions like crisis management, food supply, waste removal, health care, etc. Thus, transport is both dependent on other critical infrastructures and essential for a well-functioning society.

2.4 Information and Communication Technology (ICT)

ICT infrastructure includes communication systems for providing fixed and mobile telephony and Internet, but also intranets, local computers, and process control systems. In the DECRIS project we focus on the ICT systems used within electricity power supply, water supply and transportation.

Risk management is considered an important part of information security[1], and the focus of risk management activities is usually an ICT system or the ICT systems of an organisation. Often there is little statistical data available (Geer et al., 2003) and risk (likelihood and consequence) is thus usually determined based on expert opinions, considering e.g. the motivation and capabilities of attackers and current controls in place.

ICT systems are becoming increasingly important in many sectors, also within critical infrastructures (Luiijf and Klaver, 2004). It is our opinion that we currently have too little knowledge of how this influences the risk experienced in these sectors. Complicating factors includes the complexity of systems and how they are connected, rapid changes in technology and threats, the people aspect, and the need to consider intentional acts.

3.0 Risk and vulnerability analysis – the DECRIS approach

As mentioned initially, the current RVA practice is not able to capture the complexity of interdependent critical infrastructures in a satisfactory manner. The DECRIS approach to RVA proposes to conduct the analysis at two levels or phases.

In the first phase, the main issue is to screen the most severe risk scenarios. In a study conducted in Oslo (Sklet et al., 1997; SAFETEC, 2004), almost three hundred undesired events were identified. Hence, it is necessary to select only a subset of these for the detailed analysis. This process resembles the basic concept of a PHA with some extensions, however, one major challenge in a PHA is the assessment of consequences of an undesired event. Either we could specify the "average" consequence, or in order to highlight the severe consequences, we might rather specify a

[1] Examples of standards and methodologies that describe risk management related to ICT is OCTAVE, ITIL, ISO/IEC 13335, AS/NZS 4360 Risk Management and the NIST Risk Management Guide for Information Technology Systems.

"worst consequence".

The choice of consequence assessment will influence the way we assess the frequencies of the undesired event. If we choose the "average" consequence we need to assess the frequency of the undesired event independently of what would be the effect after the event. However, if we choose to assess a "worst case" consequence, the frequency of the undesired event should only cover the situations where the undesired event will develop in a very severe manner, i.e., a much lower frequency. Since the results of RVA analyses often are used for emergency preparedness planning, we find it most relevant to use a "worst case" approach.

In DECRIS, we are assessing several dimensions, e.g., safety, economical impact and loss of services, in the same working sheet, which makes the frequency assessment difficult in a "worst case" scenario. A proposed way to overcome this problem is to carry out the frequency assessment in two steps: First, we assess the "average" frequency of the undesired event, and then we separately assess the conditional probability that the undesired event results in a "worst case" scenario.

A PHA is usually focused on "undesired events". In order to identify risk reducing measures we need to link the undesired event to the physical infrastructure or services. We have therefore specified a procedure to link so-called safety critical functions (SCF[2]) to the undesired events, which in our DECRIS methodology is denoted "main events". This procedure is based on ideas from the BAS 5 project (Henriksen et al., 2007). Very often several SCFs are linked to one main event, and this enables us to get a first impression of the relationships between the SCFs.

The extension from a traditional PHA by introducing conditional probabilities and the explicit link to the SCF require a computerized tool. A tool may, e.g., link the risk contribution from each SCF and facilitate viewing the events or SCF's in a risk matrix etc. The InfraRisk tool has been developed for this purpose.

Based on the results from the screening phase, some scenarios are select for a detailed analysis. In phase two the aim is to get a more detailed insight into the interdependencies between the various SCFs. This will involve fault- (FTA) and event tree analysis (ETA), flow line networks, etc. The InfraRisk tool supports simple FTA and ETA, and it is a future objective to make interfaces between the InfraRisk tool and more advanced tools that treat network structures.

The DECRIS process of a RVA consists of the following steps:

1. Establish event taxonomy and risk dimensions
   a. Establish a taxonomy (hierarchy) of unwanted events. The DECRIS taxonomy has the following main event categories: Natural events, Technical/human events (error/accident), and Malicious acts.
   b. Decide on the consequence dimensions used to analyze the unwanted events. DECRIS defines the following consequence categories: Life and health, Environment, Economy, Manageability, Political Trust, and Availability of delivery/supply of infrastructure.
   c. Calibrate risk matrices. The unwanted events are described with a probability category and a consequence category for each consequence category. These categories have to be established, and a discussion is needed to calibrate the resulting risk matrices.
2. Perform a simple analysis (like a standard RVA/PHA):

[2] The physical asset like water pipeline system, water treatement, energy production plant are example of physical SCFs. The fire brigade and the police are example of non physical SCFs (NOU2006:6).

   a. Identify all unwanted (hazardous) events.
   b. Assess the risks related to each unwanted event. In the simple analysis, the two dimensions "Life and health" and "Availability of delivery/supply of infrastructure" are considered.
3. Select events for further detailed analyses. Potential candidates have usually high risk. In DECRIS specific information has been provided to support the selection, such as if the event has a gross accident potential, if there are relevant dependencies (in SCFs), and if there are communication challenges related to the event.
4. Perform detailed analysis of selected events. The course of events and various consequences are investigated in more detail. These analyses shall include :
   i. Evaluation of interactions and other couplings in between the infrastructures, and how this affects the consequences of the unwanted events.
   ii. Evaluation of vulnerabilities (e.g. critical junctions or week barriers).
   iii. Suggesting and evaluating risk and vulnerability reducing measures.

The DECRIS' methodology development faces several challenges; some were briefly mentioned in the introduction. Critical infrastructures are *large and complex systems*, including producers and vendors, customers, physical networks bringing the service from the producer/vendor to the customer and operational and control systems providing efficient and safe service. This means that the infrastructures have technological, as well as human and organizational aspects, mechanical devices and logical ICT infrastructures, spanning from international networks to components in single households. Thus, determining the system boundaries and the level of the analyses are of major importance, as well as recognizing that consequences of an unwanted event may be substantially different to the system owner than to the society.

Another challenge is *access to the competence and information* about system architecture, sub systems and components, existing safety measures, users of the system and so on. Collection of data may be resource demanding and time consuming, which means that involvement of system experts is necessary.

The distinction between *safety and security* introduce methodological challenges. The traditional risk analyses have been developed and used, e.g, in the nuclear power and the petroleum industry, to assess frequencies that are based on statistics and consequences of technical failures. Using the same type of frequencies for malicious acts is difficult, due to lack of statistics and balanced information (Line et al., 2006).

Consequences may vary between the infrastructures. In a cross sector approach, the categories have to be valid for all infrastructures, requiring a *common scale* so that the loss in one infrastructure is comparable to another. One solution may be to calculate the losses in economic value, however, some losses may then be difficult to determine, such as the value of a human life. Consequences may also cause other events leading to new consequences: An unwanted event in one critical infrastructure may quickly influence on other infrastructures. Determining the level of consequences is important, as well as deciding whether sequential consequences and *interdepencies* should be taken into consideration; aspects that are very difficult to include in traditional RVA.

As previously discussed, it may be difficult to make decisions regarding risk reducing efforts. Most often, the starting point for implementation is cost efficiency, but in many cases it turns out to be difficult to estimate such figures. Sometimes the decision process ends up in a non-optimal solution, because it may be influenced by other conditions, e.g., political negotiations.

4.0 Case study of the City of Oslo – preliminary results

Most often, methodology development becomes more effective if relevant stakeholders and decision makers are involved. Practical use of the results is usually enhanced and increased knowledge about important decision processes is gained. In the DECRIS project, the City of Oslo and representatives from the municipality's Emergency Preparedness Group are involved in a case study. The preliminary results from the case study are related to events in the categories electricity supply, water supply, transportation, and common natural events. ICT aspects are included within the first three groups. The events have been selected based on previous risk analyses (Sklet et al., 1997; SAFETEC, 2004) and through discussions with the stakeholders involved.

4.1 Electricity supply

A total of 14 undesired events related to the electricity supply have been analysed, potentially leading to wide-area interruptions. Neither of these is found to be of high risk to human life and health or to have a gross accident potential, even though several events cause severe economic losses, so far a consequence dimension not considered in DECRIS. The analysis has found some interdependencies between the infrastructures (SCF), the ICT and the electric power system, in particular.

The other infrastructures depend to a large extent on electricity supply. Thus, one outcome of step three in the DECRIS process is to further study the consequences of loss of electricity supply for water and sewage, transport and ICT systems.

4.2 Water supply

Nine undesired events have been assessed related to the water supply system. Only two events have dependencies to other infrastructures, and only one event is classified as a high risk event. If polluted water is supplied from the basin, the potential consequences may be severe, as it may be difficult to discover the pollution before people become poisoned and ill.

Several of the water supply events have public communication challenges, like the event discussed above.

4.3 Transportation

Malicious acts are included within the 23 undesired events related to transportation. The systems analyzed are road and rail. The high risk events regarding life and health are fire in a road tunnel, fire in a rail tunnel and bomb on a train.

Several events have dependencies to other infrastructures (SCF), especially to ICT, which is affected as a result of the event.

4.4 Natural events

Only two undesired events are included in this category; landslide and flooding[3]. None of the events considered in DECRIS are site specific, but both of them have dependencies to critical

[3] Natural events are believed to be dealt with in AdaptCRVA, another SAMRISK project focusing on risks due to climate change.

infrastructures. Flooding is considered to have the least risk to human life and health.

4.5 Selection of events for detailed analysis

Four undesired events from the above mentioned categories have been selected for further detailed studies (step four in the DECRIS process). The focus in the detailed analyses will be more on consequences, than on the causes. The selection has been based on the following criteria (A-E):

- A – All relevant infrastructures shall be involved in at least one scenario.
- Related to causes of the scenarios:
  - B_1 – At least one scenario shall be caused by a natural event (e.g., flood, storm).
  - B_2 – At least two scenarios shall be caused by a technical/human event.
  - B_3 – At least one scenario shall be caused by a malicious act.

However, the focus in the detailed analyses will be more on consequences, than on the causes.

- C – The events shall have a serious consequence. At least one scenario shall have a major accident potential.
- D – The scenarios shall illustrate interdependencies between the infrastructures.
- E – At least one scenario shall be feasible for analysis of decision processes, including risk communication.

Table 1 lists the events selected for detailed analyses and shows that all the decision criteria have been fulfilled. The selection of the events and the development of the criteria have been based on discussions with stakeholders and infrastructure owners.

Table 1: Selection of events and fulfillment of criteria.

Event	A	B	C	D	E
Loss of main water supply from Maridalsvannet - Case: Consequences for Ullevål hospital	Water	B_2/B_3	X		X
Loss of electricity supply (main transformer stations/regional grid/)	Electricity	B_1/B_2		X	X
Fire/explosion at Sjursøya	Transport	B_2/B_3?	X		X
Event regarding culvert – Case: Culvert Oslo S	Electricity, transport, ICT	B_2		X	X

5.0 Discussion and further work

The case study with the City of Oslo has created a very good process with many fruitful discussions, fully demonstrating the need for RVA analyses of critical infrastructure *across sectors* (involving expertise from all involved infrastructures). The preliminary results show that there are dependencies between the undesired events, and that there really is a need for analyzing the infrastructures and the undesired events collectively, and not separately as most often are done in similar analyses.

The discussions have revealed, e.g, the need for the infrastructure owners to gain knowledge of each other's systems, for example regarding site specific information about cables and pipelines. A typical situation, which is addressed in the event regarding the culvert, is what happened at Oslo S last year, when an entrepreneur unwarily broke a cable when digging a ditch, and the cable break

led to short circuit and fire, further paralyzing the region's rail traffic and transportation systems for 20 hours, and internet systems for about 10 hours (DSB, 2008).

DECRIS is halfway completed, which means that we cannot make any conclusive comments yet. However, the experiences made so far reveals that there is a need for improved systematics in order to facilitate the system decomposition during the analyses. Grouping the events and assessing causes and consequences may sometimes end up in a messy situation due to identification of an "endless" number of undesired events, sometimes overlapping, and sometimes one being the consequence of another one - being the cause of the first one.

Considerable work remains to complete the detailed analyses (of the selected four unwanted events), but progress has been made, and ways to identify/describe dependencies are tested out. Knowledge of the systems and their functional capacity in a normal use situation has been attained. An analysis often requires information about the systems' maximum capacity and how they respond to changes caused by undesired events. Use of network models for transportation, water, and electricity supply will enhance the DECRIS' analysis process

The DECRIS project is to be completed by June 2009. In the year to come, we will focus on step four in the development process, i.e., the detailed analyses of the four selected events (Table 1).

Acknowledgements

DECRIS is a project included in the SAMRISK research programme, funded by the Norwegian Research Council. We would also like to acknowledge Oslo municipality and the Emergency Preparedness Group (In Norwegian: Beredskapsgruppa), and especially the Emergency Planning Agency (In Norwegian: Beredskapsetaten) for their engagement in the case study.

References

Doorman, G., Uhlen, K., Kjølle, G. H., Ryen, K., Hestnes, B. and Ween, H. O. (2006) Vulnerability Analysis of the Nordic Power System. *IEEE Trans. on Power Systems,* 21.

DSB (2008) Fire in cable culvert. Oslo Central Station (In Norwegian: Brann i kabelkulvert. Oslo Sentralstasjon 27.11.2007), Tønsberg, Directorate for Civil Protection and Emergency Planning.

Geer, D., Hoo, K. S. and Jaquith, A. I. (2003) Information Security: Why the Future Belongs to the Quants. *IEEE Security and Privacy,* 1, pp 24-32.

Government appointed commission (2006) Protection of critical infrastructures and critical societal functions in Norway (In Norwegian: Når sikkerheten er viktigst), *Report NOU 2006:6 submitted to the Ministry of Justice and the Police by the government appointed commission for the protection of critical infrastructure on 5th of April 2006.*

Henriksen, S., Sørli, K. and Bogen, L. (2007) Method for identification and ranking of critical societal functions (In Norwegian: Metode for identifisering og rangering av kritiske samfunnsfunksjoner, FFI.

IEC (1999) IEV 60050-191 Dependability and quality of service.

IEEE/CIGRE (2004) Joint task force on stability terms and definitions: Definition and classification of power system stability. *IEEE Trans. on Power Systems,* 19.

Line, M. B., Nordland, O., Røstad, L. and Tøndel, I. A. (2006) "Safety vs. Security?," Proceedings of the 8th International Conference on Probabilistic Safety Assessment and Management, *PSAM8*.

Luiijf, E. A. M. and Klaver, M. H. A. (2004) Protecting a Nation's Critical Infrastructure: The First Steps, *IEEE International Conference on Systems, Man and Cybernetics*.

Rinaldi, S. M., Peerenboom, J. P. and Kelly, T. K. (2001) Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, pp 11-25.

Røstum, J., November, V. and Vatn, J. (2008) COST Action C19 Proactive crisis management of urban infrastructure, *COST Urban Civil Infrastructure Development Domain, ISBN 978-82-536-1003-0*.

SAFETEC (2004) Oslo municipality, Emergency Planning Agency, Main report, Update of RVA analysis (In Norwegian: Oslo kommune, Beredskapsetaten, Hovedrapport- Oppdatering av ROS-analyse). Restricted report.

Sklet, S., Tinmannsvik, R. K. and Øien, K. (1997) Safety and emergency preparedness in Oslo municipality (In Norwegian: Sikkerhet og beredskap i Oslo kommune). Restricted report, Trondheim, Norway, SINTEF Safety and Reliability.