

Transport network vulnerability – which terminology and metrics should we use?

Paper presented at the NECTAR Cluster 1 Seminar, Molde, Norway, 12-13 May 2006.

Jan Husdal

Molde Research Institute
Britv 4, 6411 Molde, Norway
Tel: +47 71214289, Email: jan.p.husdal@himolde.no

Abstract

Transport network vulnerability is a relatively new field of research and to this date no commonly agreed definition or quantifiable expression of what vulnerability is exists within the academic community. This paper presents a review of road network vulnerability, seeking to synthesize different terminologies and metrics, among which: reliability, vulnerability, resilience, flexibility, robustness, and adaptive capacity.

1 Introduction

The vulnerability of road networks has been the subject of growing attention in recent years, and there are indeed many threats that can cause the road network to fail or to become severely impeded: congestion, an array of natural hazards, structural breakdowns, traffic accidents, power failures, to mention but a few.

Road networks are the backbone of modern society. Consequently, the reliability of this road network is thus a decisive factor not only in terms of market outreach and competition, but also in terms of continuity, to ensure a 24/7 operation of the community we live in. Any threat to the reliability of the road network constitutes a vulnerable spot, a weakness, that need to be addressed in order for the network not to fail, given the right (in fact: “wrong”) circumstances. This is of particular concern when considering sparse, rural networks, because what by urban standards is a minor degradation (i.e. car accident, resulting in queuing, delays and diversions) may have severe consequences if occurring in a rural setting (i.e. blocking the only access road for hours, even days or weeks).

One hazard to transportation networks that has emerged recently and what may become an increasing concern in the near future are the effects of global climate change, with extreme weather and precipitation patterns not seen before, and thus closing or degrading links that were thought invulnerable to such threats (Askildsen, 2004).

From a user point of view, what matters most in relation to a road network is the following: Can I, at the desired time of departure, get from A to B by using the intended route and means of transport, and arrive at a desired time, which would be the best case. Or, does there exist no route or means of travel at all that can take me from A to B at the desired time of departure, let alone within arriving at the desired time, which to the user would be the worst case.

From a freight hauler's point of view, a vulnerable network is a network that is easily disrupted, resulting in unpredictable stops and downtime. This is probably seen as a much larger problem than a congested and slow-moving network that is relatively stable. In the latter, there is at least some guarantee that the goods will arrive at their destination, and most important, the transport costs, though annoyingly inefficient, are still calculable and lead times are still predictable.

This paper presents an admittedly selective review of past and present research into the field of road network vulnerability, and seeks to synthesize the different terminologies and metrics, drawing on research not only from the field of transport, but also from other disciplines, in order to assemble a picture of the topics that need to be addressed.

2 Vulnerability

The vulnerability of road networks entered the research arena some 10 years ago, sparked primarily by the earthquake in Kobe in 1995, and more recently, the events of September 11th, 2001, when the threat of terrorist attacks became the hotbed of vulnerability research, and the term *critical infrastructure(s)* emerged as a buzzword in the years to follow.

Risk and vulnerability mapping as such has been part of community planning in Norway since the early 1990s, and the guidelines published by the Norwegian Directorate for Civil Protection and Emergency Planning define vulnerability as *the degree of inability of a system to cope with the effects or impact of external or internal threats and/or events* (DSB, 1994). This definition illustrates that vulnerability relates to how well a system copes with the strain that is put on it by the threats or events it is exposed to.

Aven et al. (2004) notes that cost-benefit analyses and environmental impact analyses are tools that are widely used within transport planning, but risk analyses and risk acceptance criteria are not. Risk and vulnerability as a concept and as a management tool has no marked tradition among the Norwegian road authorities or amongst the international road authorities.

In 2005, the Norwegian Ministry of Transport made vulnerability reduction an explicit target in their research strategy, stating that the transport sector is likely to be increasingly affected by the consequences of infrastructure breakdown/disruption caused by accidents, natural disasters, climate change and terrorist acts. Hence, risk and vulnerability analyses should be used across sectors to improve cost/benefit evaluations of security and contingency measures, to better understand vulnerability within and between sectors and modes, and to improve the quality and efficacy of current systems and measures (SD, 2005).

3 Reliability

Reliability per se is not a new concept, not from an engineering perspective. Robert Lusser is by many regarded as the father of reliability and 'Lusser's law' is perhaps the most quoted and used equation in reliability engineering. It defines the reliability of a series system as the combinatorial product of the individual component reliabilities. The reliability of a road network is thus determined by its weakest link(s), and the reliability of any object as such is most commonly described as the probability that this object will function (or fail) according

to an object-specific set of standards. Put very crudely, it is the ratio of observed functioning and observed non-functioning events.

Traditionally, when looking at the reliability of transport networks, it is done with a systems engineering approach. Reliability is here an expression of the probability that links within the network will function, reliability may thus be viewed as the degree of stability of the quality of service that a system offers. One major discourse on transport network reliability is found in Bell and Iida (1997); here, reliability is focused on connectivity reliability (also named terminal reliability) and travel time reliability. Nicholson et al. (2003), in addition, list and discuss encountered reliability, capacity reliability and flow decrement reliability as ways of measuring reliability.

However, as Jenelius (2006) points out, studies of transport network reliability to a large extent only seek to quantify the probability and to some degree the extent of failure, disregarding the potential for successfully handling the effects of failure, since obviously, a vulnerability only then becomes a true vulnerability if the effects of failure indeed result in severe consequences.

In the most common manner of speaking, the reliability of a transport network can be defined as the probability that one or more of its links functions, or in better said, the probability that one or more of its links does not fail to function. Vulnerability, on the other hand, represents the network's or the links' susceptibility to failure, where the term failure here expresses a considerable deviation from the normal functioning state of the link or network. A non-functioning, or at best, badly-functioning link will impose costs on the user in terms of loss of time, additional operation costs or other costs as a result of delays and diversions. Transporters of perishable goods will also experience a loss of value. These are socio-economic costs that should be taken into consideration when evaluating or measuring vulnerability (Husdal, 2004)

4 The many facets of transport network vulnerability

As several authors have lamented, Lleras-Echeverri, and Sanchez-Silva, M. (2001), Berdica (2002), Taylor and D'Este (2003) and Jenelius (2006), to mention but a few, the vulnerability of transport networks does not yet have a commonly accepted definition. What most authors do agree upon is that vulnerability should focus on the impacts of the different threats to the network and not on the threats themselves.

Ezell et al. (2000) describe an infrastructure risk analysis model, considering possible threats and potential impacts. Their model follows the commonly accepted risk assessment method of fault and event trees. Exposure and access serve as an initial measure of vulnerability that requires further investigation and assessment, implying malevolence and security threats as their main cause for concern. The model provides a systematic process to conduct vulnerability modelling, assessment and management across different infrastructures, allowing for rank-ordering of alternatives and scenario bounding.

Transport networks are susceptible to a whole battery of scenarios that can lead to an operational degradation, and in essence, a vulnerability analysis must answer the three following questions: First, "Vulnerable...where?", to assess the location within the network.

Second, “Vulnerable...to what?”, assessing the particular circumstances or external threats and their probable occurrences. Third, “Vulnerable...how?”, addressing the particular scenario and its impact and how the network may or may not cope with it.

Cova and Conger (2004) provide an excellent practitioner-oriented discourse on transport network vulnerability in relation to a number of hazards.

Transport networks can be evaluated from two sides: the supply side, and the demand side, and they can be evaluated at (at least) two levels, the individual level, for one traveller or user, and the aggregate level, for the network as a whole. Whereas reliability analyses appear to have a clear scope here, vulnerability is more diffuse, and the susceptibility to threats can take on many forms.

Du and Nicholson (1997) use performance (demand-oriented) as a measure of vulnerability. D’Este and Taylor (2003) use the term accessibility (supply-oriented). Berdica (2002) prefers the term reduced serviceability (demand-oriented), Husdal (2005) calls it non-operability (supply-oriented), and capacity (supply-oriented) is found in Chen et al. (2002). Jenelius (2006) settles on exposure, criticality and importance, referring to Nicholson and Du (1994), who describe a link as weak the more likely it is to fail, and as important the larger the consequences of failure are. If a link is both weak and important, it becomes a critical link. Weakness (supply-oriented) and exposure (demand-oriented) are also found in Di Mangi (2005), albeit Jenelius and Di Mangi differ somewhat in their definition of exposure.

Robustness (supply-oriented) and flexibility (demand-oriented) could also be introduced here. Whereas a flexible transport network will entail the possibility of route or mode changes according to the current circumstances, a robust network will entail staying on the designated route using the designated mode of transport, even in adverse conditions. Scott et al. (2005), establish a network robustness index by calculating change in travel cost associated with rerouting traffic from the unusable links. The idea behind this method is essentially the same as in Jenelius’ approach of weakness and exposure index.

The vulnerability of transport networks is undoubtedly an important issue. More important, however, may be how resilient the network is, i.e. how quickly it can adapt to changing circumstances and return to its normal state of operation. Looking at transport networks as systems, one can apply the ideas set forth in Dalziell and McManus (2004), where the resilience of organisations in face of a crisis is determined by their adaptive capacity, and where vulnerability is an expression of how easily it is pushed from one state into the other, similar to weakness above. A resilient, and hence non-vulnerable network, is a network that has sufficient adaptive capacity to easily accommodate the changes that are necessary to maintain or return to normal operations.

5 Vulnerability analysis – three different approaches

Many researchers in transport network vulnerability agree that finding a method for calculating a vulnerability index for a road network would be very helpful for the purpose of road management, road maintenance and repair, contingency planning or to assess regional or local effects of varying degrees of vulnerability within the network. The following presents 3 possible methods and is not meant to be exhaustive.

Jenelius et al. (2006)

Jenelius et al. use the increase in generalised travel costs weighted by the satisfied or unsatisfied demand when network links are closed as a measure of vulnerability for a case study in Northern Sweden, using the terms of importance and exposure, similar to Nicholson and Du (1994).

Importance reflects the significance of each link with regard to the network, and exposure reflects the increase in travel cost for a given location within the network. Together these measure provide substantial information to planners, road administrations and individual municipalities as to where the most vulnerable (exposed and or/important) links in the network are.

Di Mangi (2005)

Di Mangi obtains a link weakness index by looking at how important each link is for the overall set of origin/destination pairs, by assessing how many o/d paths share the same link, based on probabilistic path choice models for calculating the paths. By weighing the weakness index with travel demand, the link exposure index is calculated for each link.

In comparison it can be said that Di Mangi's method is more concerned with connectivity and less with increase in travel cost, and hence, Jenelius' method is more applicable in calculating the socio-economic impact of road network vulnerabilities.

LLeras-Echeverri, G. and Sanchez-Silva, M. (2001)

In this less frequently cited paper, terminal reliability as seen in Bell and Iida (1997), is extended to include a progressive failure scenario approach to identify critical links. A critical link is defined as a link where failure causes the highest increase in generalised travel cost. Using a critical scenario (CS) approach, first calculating the minimum paths, the connectivity of the centroids within the network is evaluated.

The advantage of the CS approach is a considerable decrease in the number of scenarios that need to be evaluated, compared to an exhaustive approach of calculating all possible scenarios.

6 What about multi-criteria analysis?

Husdal (2005) suggests a weighted multi-criteria decision approach, where, link closures or degradations are assessed by various categories of effect and the severity of the impact, thus allowing for the assessment of individual effects or impacts.

The figure below, adapted from Bråthen et al. (2004) shows some of the effects of a sudden and unforeseeable incident that leads to the closure of 2 selected links or routes. Note that the evaluation criteria and the increment values used in figure 4 are for illustration only. In this illustration, average annual daily traffic serves as the first criteria of demand, to assess the number of users that is affected. Second, the waiting time or delay time, or the time it takes to

drive the diversion is differentiated between light and heavy vehicles to roughly account for the difference in value of time for business and leisure trips. Third, perishable goods lose value if not delivered on time. Fourth, some business may experience a loss of profit, because important deliveries or shipments are not made. Fifth, combined with the other criteria, the time (and cost) of reconstruction of this particular link serves as an additional criteria. The number of evaluation criteria must be adapted to the scenario that is investigated. Evaluation categories A-Z are weighted on a 0-1 scale, such that the sum of the category weights equals 1. Each weight is multiplied with the impact value 1-5. With this approach it is possible to compare and evaluate a number of vulnerabilities and to find the most critical link or most vulnerable point according to the criteria used.

Evaluation Category	Impact				
	Negligible (1)	Low (2)	Some (3)	Serious (4)	Severe (5)
(A) AADT _{no}	≤ 5	6 ≤ 20	21 ≤ 50	51 ≤ 100	> 100
(B) Occurrence of event	≥ 14 years	5/3 years	1/2 years	1/3 years	1/4 year
(C) Closure/waiting time - light vehicles (W _{lv})	W _{lv} ≤ 1h	1h < W _{lv} ≤ 3h	3h < W _{lv} ≤ 6h	6h < W _{lv} ≤ 1d	W _{lv} > 1d
(D) Closure/waiting time - heavy vehicles (W _{hv})	W _{hv} ≤ 1h	1h < W _{hv} ≤ 3h	3h < W _{hv} ≤ 6h	6h < W _{hv} ≤ 1d	W _{hv} > 1d
(E) Perishable goods, loss of value	≤ 5%	6 - 10%	11 - 20%	21 - 30%	≥ 30%
(F) Businesses' loss of profit	≤ 0.5%	0.5 - 1%	1 - 2%	3.1 - 5%	≥ 5%
(G) Reconstruction time (R _t)	< 1 wk	1wk < R _t ≤ 3mo	3mo < R _t ≤ 3mo	3mo < R _t ≤ 6mo	> 6mo
(...) Other categories					

The advantage of this approach is that it is visually appealing; on the downside, at the current stage of this research, the list of possible evaluation criteria could be literally endless, and there is a large potential for personal judgement and bias in how the increments in impact are to be constructed.

7 Conclusion

The vulnerability of transport networks is not a readily quantifiable concept. However, the vulnerability itself is maybe of less concern, what is important here is the ability to deal with the impacts and to adapt to the consequences should the “right” or “wrong” circumstances occur. The reason for this is straightforward. It is because vulnerability is not a static entity and because the outcome of every individual threat or event will vary from time to time and from place to place. Strenuous conditions may not necessarily lead to a full breakdown of the network, if the network is sufficiently equipped to handle such situations or events.

Road networks are vulnerable to many (external and internal) circumstances and events, and finding a generally applicable measure of vulnerability is not an easy task. What is certain, is

that additional costs incur when people, travellers or goods do not reach their destination in space or time as intended. These vulnerability costs are both route-dependent and location-dependent, and the increase in generalised travel cost in relation to the travel demand in the network appears so far to be most feasible way to address vulnerability in transport networks.

Transport network vulnerability is a growing field of research and practice and new methods for predicting and addressing vulnerabilities are continually being developed. Globalisation is increasing, so is our dependence on transport systems, and disruptions will only become more costly and important to mitigate, as effects of disruptions ripple or cascade through interlinked networks. This will present substantial challenges to transport researchers and analysts for the foreseeable future.

8 References

1. Askildsen T.C. (2004) Ekstremværsituasjoner og transporteffekter: Næringslivets transporttilpasninger til klimaeffekter (Norwegian), Report 2004:10, Cicero Center for International Climate and Environmental Research, Oslo, Norway. English: Extreme weather and effects on transport: How business adapts to climate change
2. Aven, T. et al. (2004) RISIT – Risk and safety in the transport sector – A state-of-the-art review of current knowledge. White paper. The Research Council of Norway.
3. Bell, M.G.H.; Iida, Y. (1997) Network Reliability. In: Transportation Network Analysis, eds. M.G.H. Bell and Y Iida, pp.179-192, John Wiley & Sons, Chichester
4. Berdica, K. (2002) An introduction to road vulnerability: what has been done, is done and should be done. *Transport Policy*, 9, pp. 117-127
5. Bråthen, S.; Husdal, J. and Lægran, S. (2004) Flaskehalsar for langdistanse godstransport på veg (norwegian). Project report No. 245701, Sweco Grøner, Oslo, Norway. English: Bottlenecks in Long-Distance Road Freight Transport
6. Cova, T.J., and Conger, S. (2004) Transportation hazards. In: Handbook of Transportation Engineering, M. Kutz (ed.), McGraw Hill, New York, pp. 17.1-17.24.
7. Dalziell, E.P. and Mc Manus, S.T. (2004) Resilience, Vulnerability, and Adaptive Capacity: Implications for System Performance. Paper presented at the International Forum for Engineering Decision Making (IFED); Switzerland. December 2004
8. Di Gangi, M. (2005) Transportation Network Vulnerability Indicators for Risk Evaluation and Exposure Reduction. Proceedings of the European Transport Conference (ETC 2005), Strasbourg, France,
9. DSB (1994) Veileder for kommunale risiko- og sårbarhetsanalyser (Norwegian). English: Guidelines for municipal risk and vulnerability analyses, Norwegian Directorate for Civil Protection and Emergency Planning
10. Du, Z.-P. and Nicholson, A. (1997) Degradable Transport Systems: Sensitivity and Reliability Analysis. *Transportation Research Part B* 31 (3) pp 225-237
11. Ezell, B.C.; Farr J.V.; Wiese,I. (2000) Infrastructure Risk Analysis Model. *Journal of Infrastructure Systems*, 6 (3,) pp 114-117
12. Husdal, J. (2004) Pålitelighet og sårbarhet – et ikke-tema i nyttekostanalyser? *Samferdsel* 2/2004, s. 28-30. (Norwegian). English: Reliability and vulnerability – a non-issue in cost-benefit analyses? *Samferdsel* (Journal of the Norwegian Institute for Transport Economics, TØI), 2/2004, pp. 28-30

13. Husdal, J. (2005) The vulnerability of road networks in a cost-benefit perspective. Proceedings of the the Transportation Research Board Annual Meeting (TRB 2005), Washington DC, USA, 9-13 January 2005.
14. Jenelius, E.; Petersen, T. and Mattson, L.-G. (2006) Importance and exposure in road network vulnerability analysis. *Transportation Research Part A* 40 pp 537-560
15. Lleras-Echeverri, G. and Sanchez-Silva, M. (2001) Vulnerability analysis of highway networks, methodology and case study. *Transport* 174 (4), pp.223-230.
16. Nicholson, A.; Schmöcker, J.-D.; Bell, M.G.H. and Iida, Y (2003) Assessing Transport Reliability: Malevolence and User Knowledge. In: *The Network Reliability of Transport*, eds. M.G.H. Bell and Y. Iida, Proceedings of the 1st International Symposium on Transportation Network Reliability, pp.1-22. Elsevier Science, Kidlington.
17. Nicholson, A. and Du, Z.P. (1994) Improving network reliability. Proceedings of the 17th Australian Road Research Board Conference, pp 1-17
18. Scott, D.M.; Novak D.; Aultmann-Hall, L. and Guo F. (2005) Network Robustness Index: A New Method for Identifying Critical Links and Evaluating the Performance of Transportation Networks. CSpA Working paper 009, McMaster University, Canada
19. SD (2005) Strategi for tele- og transportforskning 2006 – 2009 (Norwegian). English: Strategy for telecommunications and transport research 2006 – 2009, Norwegian Ministry of Transport and communications
20. Taylor, M. A. P. and D'Este, G.M.D. (2003a) Network Vulnerability: An Approach to Reliability Analysis at the Level of National Strategic Transport Networks. In: *The Network Reliability of Transport*, eds. M.G.H. Bell and Y. Iida, Proceedings of the 1st International Symposium on Transportation Network Reliability, pp.23-44. Elsevier Science, Kidlington.
21. Taylor, M. A. P. and D'Este, G.M.D. (2003b) Concepts of network vulnerability and applications to the identification of critical elements of transport infrastructure. Paper presented at the 26th Australasian Transport Research Forum, Wellington, New Zealand, 1-3 October 2003.