# On the dependability of IP networks
## Results of the IPLU-II project

**Contents:**



# 1 Introduction

The motivation of the IPLU[1] project in 2006 and its follow-up IPLU-II was the concern about the dependability of the envisioned IP-based communication infrastructure. IPLU's task was to create a broad conceptual framework for considering the complex problem "Can one rely on IP technology?" and to identify and develop methods for assessing the dependability of IP networks. IPLU-II continued with selected focused topics. A special feature of IPLU and IPLU-II was their multidisciplinarity, combining VTT's expertise on communication technologies, mathematical modelling, statistics, safety-critical systems and psychology. The outputs of both projects are available on their common homepage http://iplu.vtt.fi.

IPLU-II was part of the GIGA programme of Tekes. The research effort, led by Research Professor Ilkka Norros, was made by VTT, and the other partners of the project were Ministry of Traffic and Communications, National Emergency Supply Agency, BaseN, CSC, Digita, Elisa, Finnet, Fortum, F-Secure, Nokia Siemens Networks, TDC and TeliaSonera. IPLU-II was started in February 2007 and finished in June 2009. The total volume of the project was 500 k€.

[1] "IPLU" stands for "IP-verkkojen luotettavuuden arviointimenetelmät" ("Dependability evaluation methods for IP networks"), and IPLU-II for the same plus "vaihe 2" ("phase 2").

This report summarizes the main results of IPLU-II. Each section is concluded with a short "Next steps" paragraph pointing to application possibilities and/or problems for further research.

# 2 Dependability case methodology

IPLU developed the basic ideas of a "dependability case" methodology that makes it possible to combine a heterogeneous set of relevant requirements, facts, tools, techniques etc. into an organized argumentation structure in support of a claim concerning the dependability of a network. The feasibility of this approach was tested in IPLU-II by building a rather comprehensive dependability case of the Funet network in collaboration with CSC experts running the network. The study is reported in [6], and the whole case is available at the project homepage. Here we highlight the main solutions how the case was built and make some remarks and conclusions.

At the highest level, the overall dependability claim of the network was partitioned according to the main aspects of IP network dependability identified in IPLU: availability, reliability, maintainability, controllability, invulnerability and robustness of basic protocols. Claims on high availability etc. were further subdivided into more and more particular subclaims. The evidence for support of these claims consisted of topology, availability and traffic data (our "hard" evidence) and interviews of CSC personnel (our "soft" evidence). Argumentation linking the claims to evidence was written into a graphical presentation of the dependability case.

The chosen structuring principle worked well in the Funet case. All our information concerning the dependability of the network could be included and organized in a logical way without forcing. Still more important, it was obvious how sharpening the argumentation by more evidence and more extensive analyses could happen at various points without changing the general structure. With the selected approach, similar types of issues are addressed in the same logical location, whereas qualitatively different types of issues are clearly separated from each other. Thus, specialists of different fields can contribute to a dependability case, each having a specified and well defined task in the case. Different viewpoints and argumentation results are summarized at higher and more abstract levels of the dependability case.

*Next steps:* The methodology is basically ready to be applied as a network operator's tool for (i) taking care of the dependability of a network and maintaining an overview of all its aspects, and (ii) communicating this to, for example, a regulator. VTT would be interested in collaborating in such an effort, whereas we don't consider it fruitful to develop the methodology further without a concrete application.

# 3 Monitoring of dependability

## 3.1 The tricky concept of IP-availability

In one form or another, availability is always part of Service Level Agreement (SLA). In IPLU-II the concept of availability was studied in the special case of IP networks. The study is reported in [3]. The study [3] was concentrated on the IP *service* availability, which is a different concept than the more topologically oriented concept of *network* availability which is usually formulated in

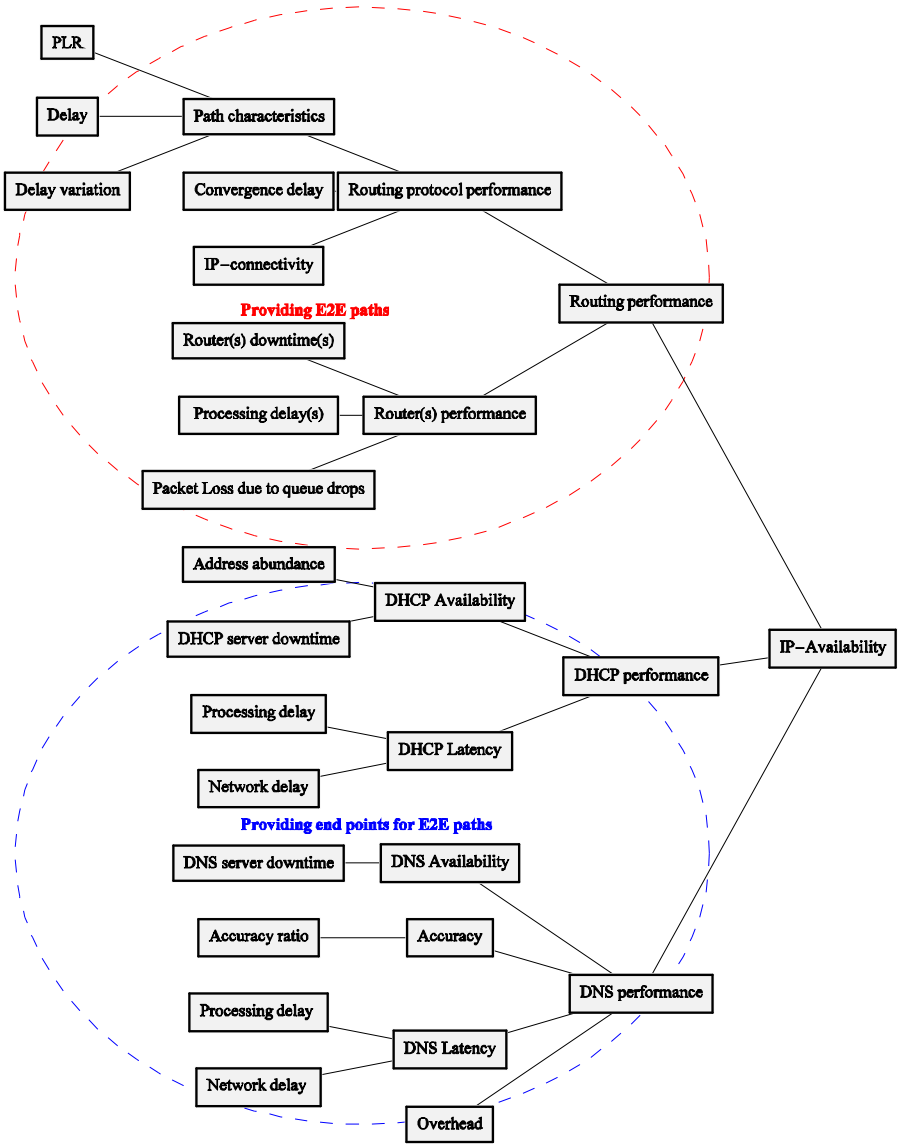


**Figure 1. Components of IP service availability.**

terms of graphs. Essentially, the work reported in [3] concentrates on IP-specific features of availability, IP-layer functions and cross-layer demands and does not aim to any kind of formula. The main idea is to split IP service availability into smaller and smaller pieces such that, in the end, everything is measurable or, at least, can be benchmarked in the service deployment phase. This is illustrated in Figure 1.

IP service availability is essentially the ability of the IP network to carry customer traffic between any valid source and destination hosts. A metric of IP service availability must be something that quantifies the disruption in packet forwarding due to failures. The base definition is the IP Connectivity metric of the IP Performance Monitoring Working Group of IETF, given in RFC 2678. However, there are some issues that remain unsolved:

1. Correlation with the customer experience? The conclusion in the study [3] was that correlation with the customer experience requires that the customer can measure/test IP-availability. This may require including DHCP and DNS performance issues in IP-availability to some extent. This is why DHCP and DNS are included in Figure 1.
2. What to do in case of service failures? This is the main motivation in the study [3]. From the customer point of view availability is just dichotomous question but from the operator point of view there are far more issues to consider. These are illustrated in Figure 1. The availability is the key part of the commercial product of the operator. Thus, in order to maintain the availability the operator must obtain fast structural and spatial information about possible threats and failures in the network. The operator needs passive and active measurement and monitoring and benchmarking methods to monitor IP-availability. See [3] for more details.

*Next steps*: Fast localization of failures, spatially and structurally, seems to require better troubleshooting tools. The new NSIS framework seems to provide a generic and flexible protocol family on top of which it is good to build new monitoring tools. VTT would be interested in prototyping new types of troubleshooting tools.

## 3.2 Monitoring of IP-TV availability

During IPLU-II, a brief IP-TV case study from the network of TDC was made. From this case study a certain type of a problem was identified, and a solution outline was proposed and reported in [4].

Consider the following scenario for monitoring the quality of multicast based delivery of IPTV. We want to know if the multicast delivery maintains the quality of the transport stream sufficiently well from the root to an arbitrary node or leaf of the multicast tree. Especially, we want to localize the possible problematic part of the tree and the delivery network. The solution to this problem was developed in the IPLU-II project and is the following: The quality of the transport stream that carries IPTV traffic is continuously measured at the root of the multicast tree. This quality information is then, periodically, sent to all those nodes and leafs of the multicast tree that are participating to the troubleshooting process of detecting the possible low quality. At each node or leaf which is participating to the troubleshooting process the same quality measurement of the transport stream is made and then compared with the information obtained from the root. This comparison then tells directly whether the part of the multicast tree from the root to the node in question is able to maintain sufficient quality or not.

*Next steps*:

There are two main problems that need to be solved for the above described distributed troubleshooting to work with IPTV. First, we must develop a suitable quality metric for the transport stream. This requires a bit stream layer model (see [4]) and utilizes the decoder. The ETSI Technical Recommendation 101 290 defines a number called Unavailable Time which, while still insufficient for the IPTV purposes, is very close to what is needed. The Unavailable Time attempts to measure the availability of the transport stream. This existing metric must be reformulated in order to work over transport streams that are carried over IP. This is a challenging issue.

The other main problem is the synchronization between the nodes that participate to the troubleshooting process. In order that the comparisons provide meaningful and reliable results the synchronization must enable the measurements of the same part of the transport stream at two different locations. There are two choices for this. The synchronization can be in time in which case NTP could be used. A possibly better way though would be to synchronize the measurement points to the stream itself. In this case the stream acts as a clock and the synchronization is then, essentially, made to the frequency of the stream. In practice the availability of the both ways of synchronization would be the best. First, using time synchronization offered by NTP some fast results are obtained and then, after the synchronization to the stream, some more exact results can be achieved. VTT would also be interested in prototyping the above described IPTV monitoring scenario.

# 4 Network reliability analysis

## *4.1 Protection by multiple MPLS spanning trees*

Data delivery in a MPLS core network motivated an IPLU-II case study, in which two principles of delivering data are compared in a network in terms of tolerance to link and/or node failures. This analysis can be used in designing the topology of a future network and in selecting the actual data delivery method.

The task is to deliver data from one source to six destinations in a network. If all non-failed destination nodes receive the data, the task is considered successful. The two principles of data delivery are: (i) multicast data from the source twice in the network by using two independent (i.e., no links in common) spanning trees and (ii) multicast data from the source only once and use fast rerouting, if link or node failures occur.

The approach of multicasting twice is demonstrated by two possible spanning tree pairs as the results depend on the pair of trees used. In general, two spanning trees can tolerate any one component failure. Once this delivery has been set up, it requires no additional actions in case of component failures. However, the usage of the network capacity is larger than necessary.

The two spanning tree method is compared with the following global repair approach: “One spanning tree is selected for delivery. If there are link or node failures that influence the used spanning tree, a new spanning tree is selected. For any 1-element or 2-element failure event, there is a predefined spanning tree to be used.” This approach is superior in resistance to 2-element failures. Also, the use of network capacity is optimal, as data is delivered only once. However,

spanning trees corresponding to each failure event need to be pre-calculated and stored. The needs of failure detection, signaling and real-time traffic should to be identified in this approach.

*Next steps:* It is also possible to select pairs of spanning trees optimally according to some criterion, e.g., giving nodes varying importance in terms of data delivery. Multiple spanning trees can be used in traffic balancing as well. In the use of one spanning tree the technical requirements need to be identified. However, the storage and computational power of routers increase all the time, so this approach can be expected to become feasible in the future, if the advantages of multiple trees are not needed.

### 4.2 On/off process modelling of multiple failures

The basic way to model the functioning of a system with built-in redundancy is to divide it into binary (on/off) components that either work or not, and to specify its so called structure function that tells for each component state configuration whether the system works or not. The probability that the system works can then be expressed in terms of the probability distribution of component states. In a highly dynamic system like a large communication network, static modelling of component reliability by a single probability number is insufficient, since the temporal behaviour, e.g. downtime durations, is of great interest. IPLU-II modelled the functioning of network components (links, routers) by stationary on/off processes with arbitrary distributions of on-period (uptime) lengths and off-period (downtime) lengths. The analysis of ping data from Funet routers suggested that the downtime distributions are heavy-tailed and could be modelled by Pareto distributions, whereas the uptimes were described sufficiently well by constant failure rates (corresponding to exponential uptime distributions).

Such processes are often applied in teletraffic modelling but surprisingly seldom so far in reliability theory. The Palm theory of stationary point processes [1] provides an elegant tool for working with on/off processes. In particular, an explicit formula for the distribution of joint downtimes of two or more components could be derived assuming only the independence of components. Combined with the presentation of downtime distributions in the form of downtime-frequency curves, introduced already in IPLU [8], on/off process modelling was shown to provide a natural and tractable framework for network reliability analysis. It was already applied in IPLU-II to quantitative comparison of reliability improvement strategies, see Section 5.2 below.

*Next steps:* The theory developed so far is based on the assumption of independence of component processes. The modelling of component dependences requires novel theoretical contributions. VTT is starting collaboration on this topic within the Euro-NF network of excellence.

## 5 Cost of and strategies for the improvement of dependability

### 5.1 On the cost of dependability

IPLU-II made a comprehensive study [9] of various methods to enhance the dependability of an all-IP network and considered the capital and operational expenses caused by the use of those methods. At first, different perspectives to the dependability of a packet switched network were identified and

goals of each viewpoint compiled. Then, a layered model for dependable communication was introduced and methods to increase dependability on the given layers were discussed. Finally, simple formulas were given to estimate additional Capex and Opex, caused by the different methods.

Methods to be used on the various dependability layers were classified to redundancy, network control, design activity, OAM activity and purchasing activity methods. Some other methods were also discussed. The redundancy methods, e.g. duplication of network equipment, are cost sensitive causing usually clear increase of both Capex and Opex. The network control methods may require purchase of new devices, training of personnel and hiring of new employees thus leading to clear increase in both Capex and Opex. Some other control methods may require only activation of an existing feature in the network devices, thus causing no additional expenses.

Design and purchasing activities were found to cause no additional expenses, because proper design and purchasing processes should already cover all that is needed to maintain high dependability. However, sharpening of the existing design and purchasing processes may be needed. OAM activities to increase dependability may require only modifications to the existing OAM practices, causing practically no extra expenses, or there may be need for new OAM equipment, training and new personnel in which case both Capex and Opex go up clearly.

Other discussed methods (topology, location of networking devices, agreements, history and alternative technology), may produce substantial increase in Capex and/or Opex. The use of resilient ring and mesh topologies is an example of Capex intensive methods. Agreements to increase dependability are a good example of Opex intensive methods. The highest cost increase is faced with the alternative technology option. It offers the best solution to avoid shortcomings of the IP networks, but within a short time frame results in the highest cost.

## 5.2 Modelling of reactive and proactive strategies for reliability improvement

Preventing failures in advance, repairing the failures faster, and changing the topology to be more resilient are three main principles of improving the reliability of a network. IPLU-II considered these principles as three different reliability improvement strategies for a network that was defined solely in terms of its links and routers and was described by an on/off process model as defined in Section 4.2.

A proactive strategy means working for avoiding failures. For example, one could do additional checking of network configuration parameters before the parameter change is performed. In this way, a potential failure may be prevented. Proactivity was modelled as decrease in the failure intensity of components.

A reactive improvement strategy focuses on repairing components or network functionality faster, when a failure occurs. For example, a network operator may wish to make a new SLA agreement that enforces faster repair of failures. This could reduce the minimum duration of failures, because a repair would have a higher priority and actions would be initiated earlier than before. A reactive strategy in connected to the durations of failures and it was expressed in the model in two ways, by changing either the minimum duration of a failure or another parameter of the component downtime distribution.

The third kind of improvement, a change of topology, is by nature proactive but modelled in a different way than above: now the modification of the model happens in the structure function, whereas the failure rates of components may remain at their previous levels. Nevertheless, either the failure of some network elements does not any more constitute a failure event in terms of the structure function, or the number of access routers affected by the failure event is reduced.

As the developed modelling framework can accommodate strategies for improving reliability, it became possible to compare different strategies quantitatively. The effects of proactive and reactive strategies were demonstrated in [5] using downtime-frequency curves. First, the modelling framework gives understanding of heterogeneity in reliability and points to weak *vs.* strong parts of the networks. When the knowledge on network reliability is increased it is natural to ask: "What should one do to improve the reliability?" Reliability is always a question of cost effectiveness, i.e., where to invest in order to get the best possible gain. The developed reliability model can be used to give guidelines. Reliability analysis can be done for fictive network topologies, if improvement is sought from a better topology. Alternatively, the reliability properties of network components can be altered as demonstrated in the report to correspond to either proactive or reactive strategy to reliability.

The strength of the modelling method is in exploring all possible joint failure cases. It combines the design properties of the network (topology) to historical data, which is used to estimate the reliability of components and probabilities of failure cases. In addition, one can easily proceed from a reliability approach to a risk approach to take into consideration the losses caused by temporary unavailability.

*Next steps:* Studies on the costs and strategies of improvement of network dependability should be continued toward a "network risk theory", a theoretical framework for the quantification of risks in networking.

# 6 Human factors of network operation

It seems to be a common view in the networking domain that a high percentage of network failures are caused by human errors. Therefore it is highly interesting to know what happens "behind the scene", where experts with various qualifications work continuously to keep the "invisible" infrastructure functioning. IPLU-II interviewed 20 people operating the networks of Elisa, resulting in an empirical material of 500 pages of transcribed protocols. The answers were analysed applying an approach developed at VTT for the study of experts' work in high-tech environments. The four research questions of the study were formulated as follows:
1) How do the actors perceive the network as the object of their activity?
2) What kind of skill, knowledge and collaboration requirements does the network operation work set?
3) How do the network operators act on the network?
4) What is the impact of human errors on the dependability of the network?
The background, results and conclusions of the study are presented and discussed in detail in [7]. Here we summarize only the results of a so called core-task demand analysis of network operation work, the interviewees' thoughts on the role of human errors, and some general conclusions from the study.

## 6.1 Demands of network operation work

The special work demands in high-tech environments that are intrinsically implied by features of the work domain can be generally classified as being related either to its (i) dynamics, (ii) complexity, or (iii) uncertainty. These three dimensions turned out to cover and structure the features of the object of communication network operation (CNO) very well (Figure 2; for details, see [7]). Mastering these features requires many kinds of skill, knowledge and collaboration resources as well as certain emotional resources. The obtained core-task demand structure is summarized in Figure 2.

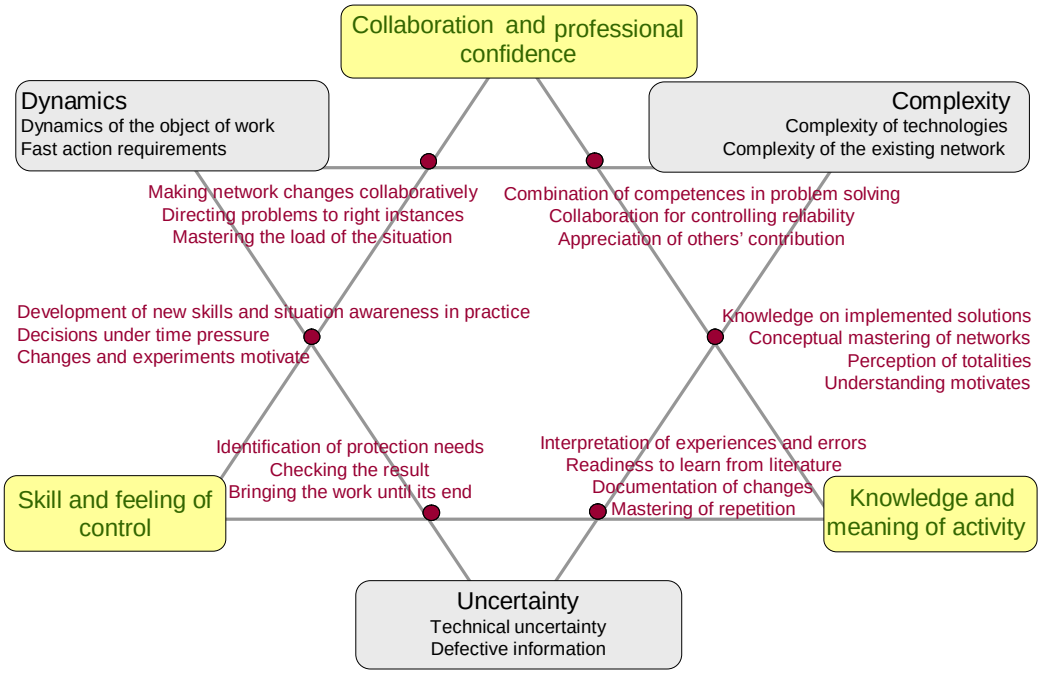


**Figure 2. Core-task demands of CNO**

## 6.2 The role of human errors

The majority of the interviewees, though not all, considered the impact of human errors on network failures as remarkable. Erroneous acts were found possible at two levels: individual level and organizational process level.

As regards the work of an individual network operator, hurry, stress, taking care of several jobs simultaneously and night work were identified as situation factors increasing the vulnerability of work performance. Two error types identified in work performances were

- lapses and confusions, in particular with configuration and with the allocation of subcontractor jobs
- errors in reasoning at configuration and planning

The vulnerability of performance at general level seems to be caused by factors acting at the level of habits and culture, like

- meaningless repetition of performance, and slackening of the control of activity during the work
- neglect of the use of knowledge or instructions
- weakening of interest and motivation.

On the other hand, many problems were less connected with the performance of individuals and could thus be alleviated by changes in processes, customer solutions, working habits and education. Errors were said to result from circumstances like defective documentation of implemented solutions, defective consideration of the effects of changes, incompleteness of the implementation of changes, neglect of checks and unpredictabilities connected with new solutions. Defects in knowledge were also mentioned as a source of errors. Excessive tailoring of customer solutions was considered much more error-prone than favouring a set of standardized solutions. Learning from errors is accentuated by their repetition, but, on the other hand, often hindered by their latency.

## *6.3 Some conclusions from the study*

First, the social importance of the networking branch and network operation work is increasing as the ubiquity of Internet access is becoming an integral part of the common technological environment. The social appreciation of CNO work deserves to be heightened.

Second, a combination of proactive and resilient ways of acting is needed in the organization and processes of CNO work. Whereas planned acts upon the network should be prepared as carefully as possible, preparedness to on-line problem-solving prompted by unexpected network failures is an integral part of CNO work.

Third, CNO work is also socially highly networked by its nature, and communication and collaboration over organizational boundaries is a challenge that needs attention. A socio-technical approach to the network should be developed. We also noted that a customer-centric way of acting seems to be gaining momentum - the network exists for its customers also in the minds of the experts.

*Next steps:* Fault diagnosis and recovery processes should be observed and studied as they happen in CNO work practice. This would be valuable not only for the development of good work practices but also for the development of better tools for network management.

# References

[1] F. Baccelli and P. Bremaud. Elements of Queueing Theory. Springer Verlag, Berlin, 2003.

[2] IEC 60812. Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA). International Standard.

[3] J.Kilpi. IP-Availability and SLA. International Workshop on Traffic Management and Traffic Engineering for the Future Internet (FITraMEn 08). Porto, Portugal, 11 - 12 Dec. 2008.

[4] J. Kilpi. Enabling distributed fault diagnosis in multicast-based IPTV delivery. Technical report, available from http://iplu.vtt.fi.

[5] P. Kuusela, I. Norros and P. Raatikainen. Report on modeling reliability of an IP-network and strategies for improving the reliability. Technical report, available from http://iplu.vtt.fi.

[6] I. Norros, P. Kuusela and P. Savola. A Dependability Case Approach to the Assessment of IP networks. The First International Workshop on Dependability and Security in Complex and Critical Information Systems (DEPEND2008), August 2008. (Available from IEEE Xplore Digital Library.)

[7] L. Norros, I. Norros, M. Liinasuo and K. Seppänen. Human activity in communication network operation - an analysis of the operating personnel's work. VTT report, to appear, 2009.

[8] I. Norros, U. Pulkkinen and J. Kilpi. Downtime-frequency curves for availability characterization. The 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN2007), 2007.

[9] P. Raatikainen. Cost to build dependable all-IP networks. Research report VTT-R-09852-07, available from http://iplu.vtt.fi, 2007.