



# Dependability Case of FUNET's core network

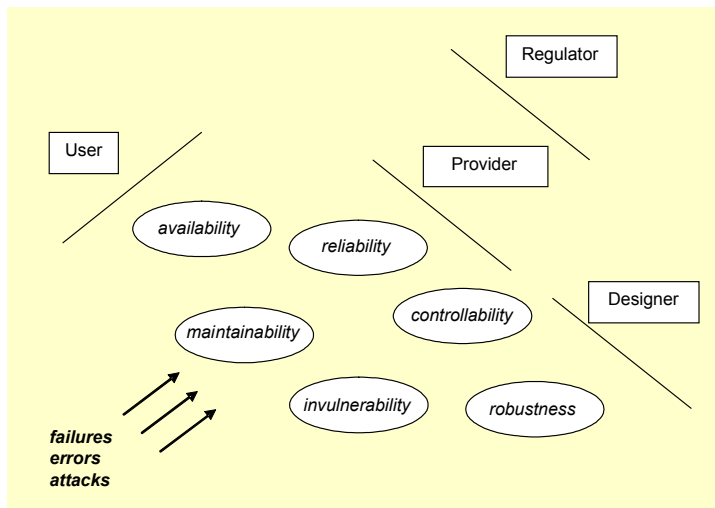
Ilkka Norros, Pirkko Kuusela and Ilkka Karanta  
VTT, Technical Research Center of Finland  
firstname.lastname@vtt.fi

Pekka Savola  
CSC - Scientific Computing Ltd.  
firstname.lastname@csc.fi

# Outline

- Concept of dependability in IP networks
- Dependability case methodology
- Case study: dependability of Funet's core network
- Discussion

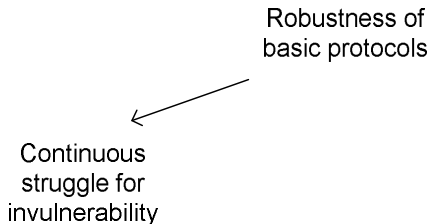
# Actors and aspects of IP dependability



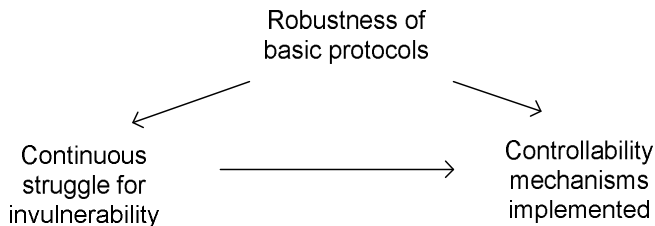
# The concept of dependability in IP networks

Robustness of  
basic protocols

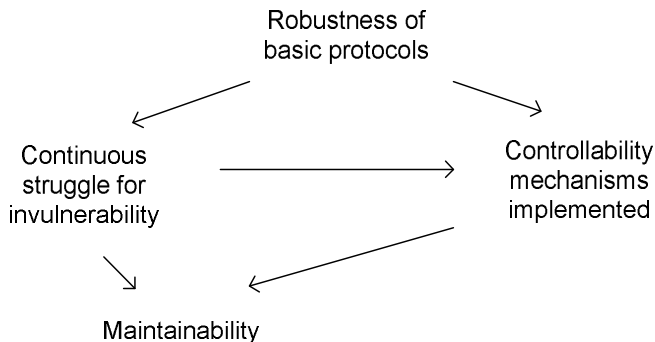
# The concept of dependability in IP networks



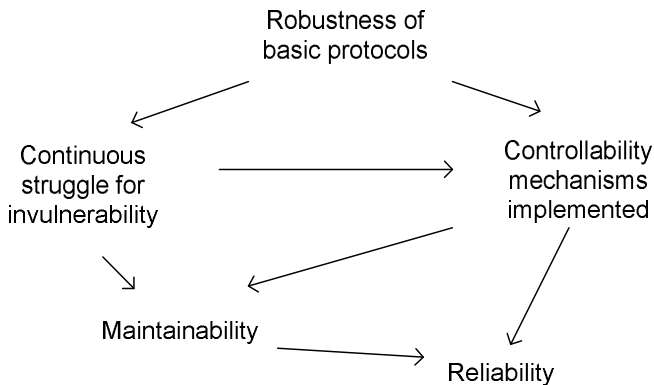
# The concept of dependability in IP networks



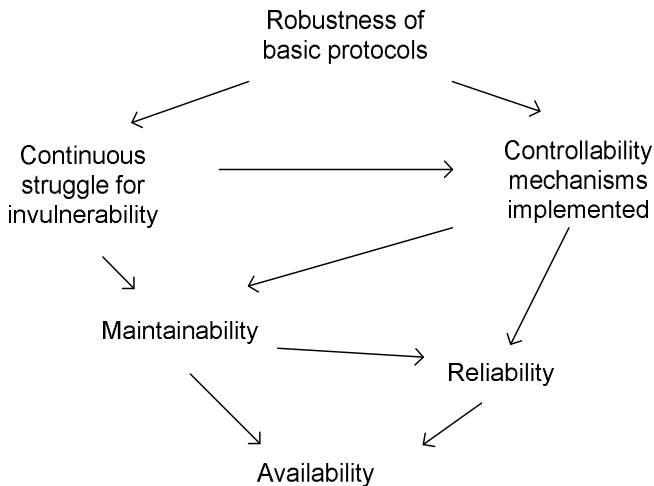
# The concept of dependability in IP networks



# The concept of dependability in IP networks



# The concept of dependability in IP networks



# Outline

- Concept of dependability in IP networks
- *Dependability case methodology*
- Case study: dependability of Funet's core network
- Discussion

# Dependability case

- safety case  $\rightarrow$  dependability case
- safety cases are standard tools in safety critical industries
- *A documented body of evidence that provides a convincing and valid argument that a system is adequately dependable for a given application in a given environment.*
- tool for assessment and approval, but also for taking care
- showing what depends on what is important
- meant to be living
- emphasis on understandability and traceability

# Elements of dependability case

*GRAPHICAL VISUALIZATION* of argumentation structure

- *CLAIMS*
- *EVIDENCE*
- *ARGUMENTS*

# Elements of dependability case

## *GRAPHICAL VISUALIZATION* of argumentation structure

- *CLAIMS*
  - goals, or statements about system or subsystem
- *EVIDENCE*
  - facts about system: general knowledge, soft or hard data, test results
  - explicitly registered and available
- *ARGUMENTS*
  - provide support to claims based on evidence
  - deterministic, probabilistic, qualitative
  - give the meaning of the data in the context of claims

# Evaluation process

CLAIM

How well does  
the argument  
support the  
claim?

↑  
weak normal strong

ARGUMENT

Is evidence of  
high quality and  
relevant to the  
argument?

↑  
weak normal strong

EVIDENCE

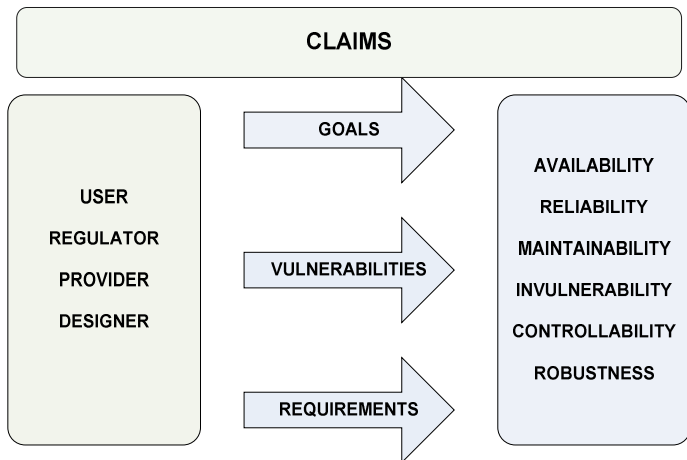
# Outline

- Concept of dependability in IP networks
- Dependability case methodology
- *Case study: dependability of Funet's core network*
- Discussion

# An experimental dependability case of Funet

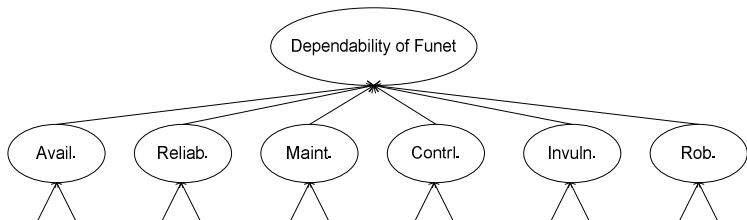
- Testing the idea with a real network
- What evidence is available?
  - Does it provide needed information?
- How easily do network structures adapt for classical reliability analysis?
- Generality over speciality, wide coverage
- **NOT** the real dependability assessment, but possibly a way to make one

# Where do claims come from?



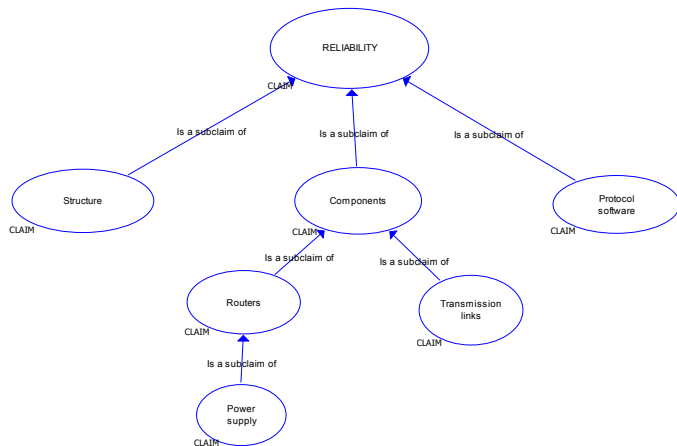
# Chosen claim structure

according to aspects of dependability

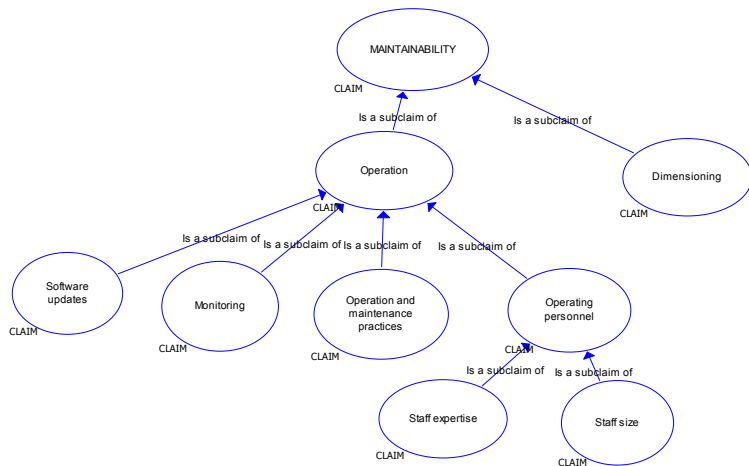


- General high-level claims, e.g., “Availability is high”
- 4 levels of sub-claims, more specific
- Real case would have explicit target values

# Claims on reliability



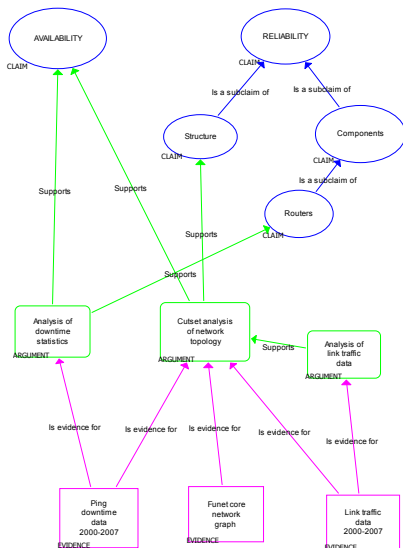
# Claims on maintainability



# Evidence and arguments

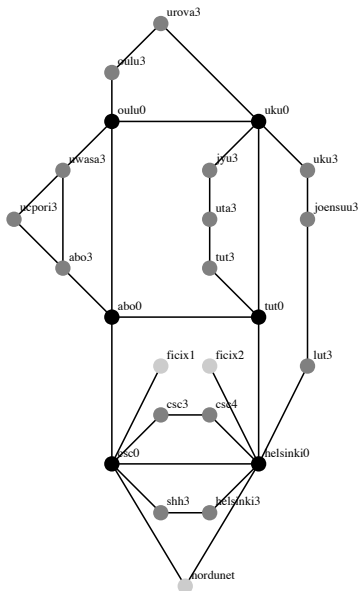
- Evidence:
  - 3 interviews
  - core network topology
  - ping data
  - link traffic data
- Arguments:
  - qualitative argumentation (most common)
  - analysis of downtime statistics
  - cutset analysis of network topology
  - analysis of link traffic data
- What was not available:
  - Service Level Agreements
  - other non-public information

# Illustration of reliability argumentation



# Cutset analysis, idea

- topology (physical = logical)
- routing rules
- chosen structure function:  
Funet OK if
  1. connected
  2. link to Ficix
  3. link to NorduNet



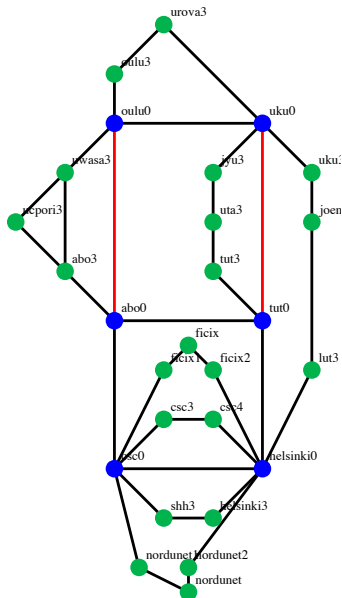
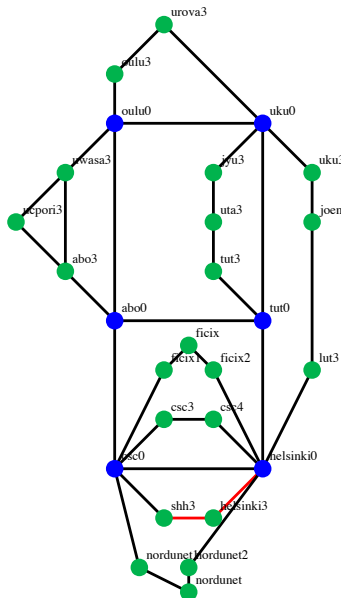
# Cutset analysis, example of results

theoretical failure cases, 2 links or nodes fail

Failures:

failed element		how many cases
links	nodes	
2	0	23
1	1	49
0	2	26
total		98

2 links fail, 23 cases



# Cutset analysis, remarks

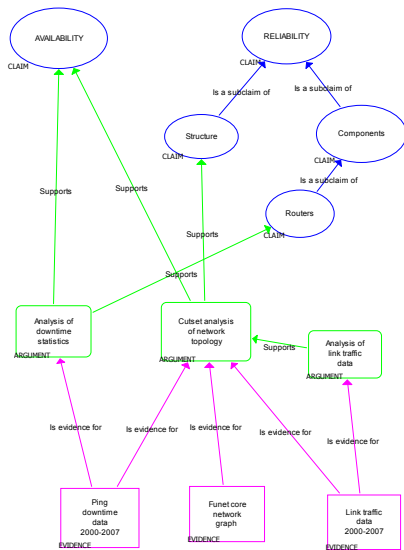
Can do more:

- combine probabilities & link loads  $\Rightarrow$  risk estimates
- risk = failure probability  $\times$  lost traffic

What if network is large?

- can not list all cases
- can use graph spectral theory to find the most vulnerable links for worst partitions of network
- huge networks??

# Illustration of availability argumentation, downtime statistics



# Analysis of downtime statistics

CSC ping data:

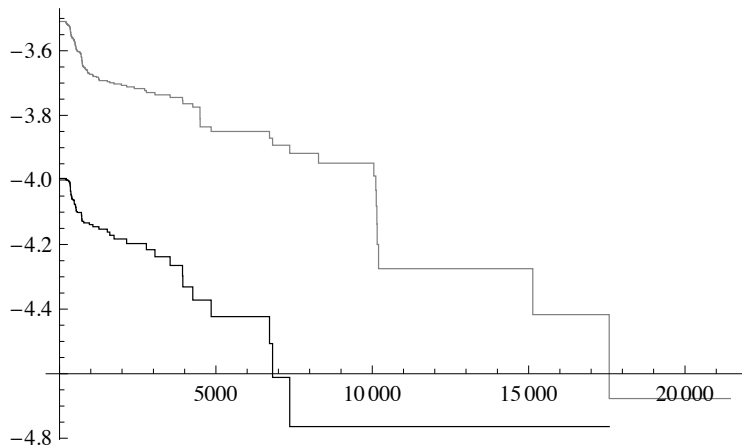
- 6 core routers and customer's sites
- 5 pings in 1 min intervals
- no response to any  $\rightarrow$  site marked down
- August 1, 2000 – July 31, 2007
- 310 records, 55 marked planned  $\rightarrow$  255 in analysis
- downtime cluster = max continuous union of  $\geq 2$  downtimes
- 170 of 255 downtimes were in 35 clusters
- 2 clusters contained 14 downtimes

remarks

- individual downtimes  $\neq$  independent rare events
- not very good for evaluating availability

# Downtime frequency curves for core routers

$\log_{10} P(\text{on-going downtime} > t \text{ sec})$



gray: all data, black: clusters censored

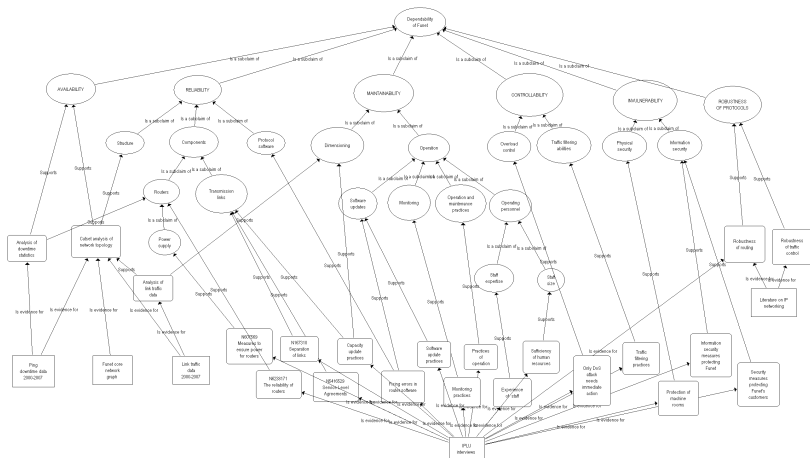
# Qualitative argumentation

18 qualitative arguments

examples:

- meets dimensioning, controllability, maintainability claims well, availability high
- traffic well predictable
- CSC monitoring during office hours, automatic alarms
- no full own control on physical security

# Complete dependability case



Created with GSN4j Educational Edition - valid for non-commercial teaching and research purposes only

# Perspectives of dependability case methodology

- Tool for taking care of dependability
- Good in visualizing dependability
- Technical arguments can be integrated into qualitative arguments
- Allows structuring

Will this work

- When the network is larger/ more complex?
- When assessment is more serious?
- Can monitoring be combined to dependability case? Some aspects are stable, some evolve all the time (network usage)

# How to benefit from a dependability case?

- Communicating dependability
  - user – provider relation
  - provider – regulator relation
- Management of dependability
  - general picture, internal tool
  - can be used in training
- Improvement of dependability
  - showing weak and strong parts
  - change in time