Dependability Case of Funet's core network

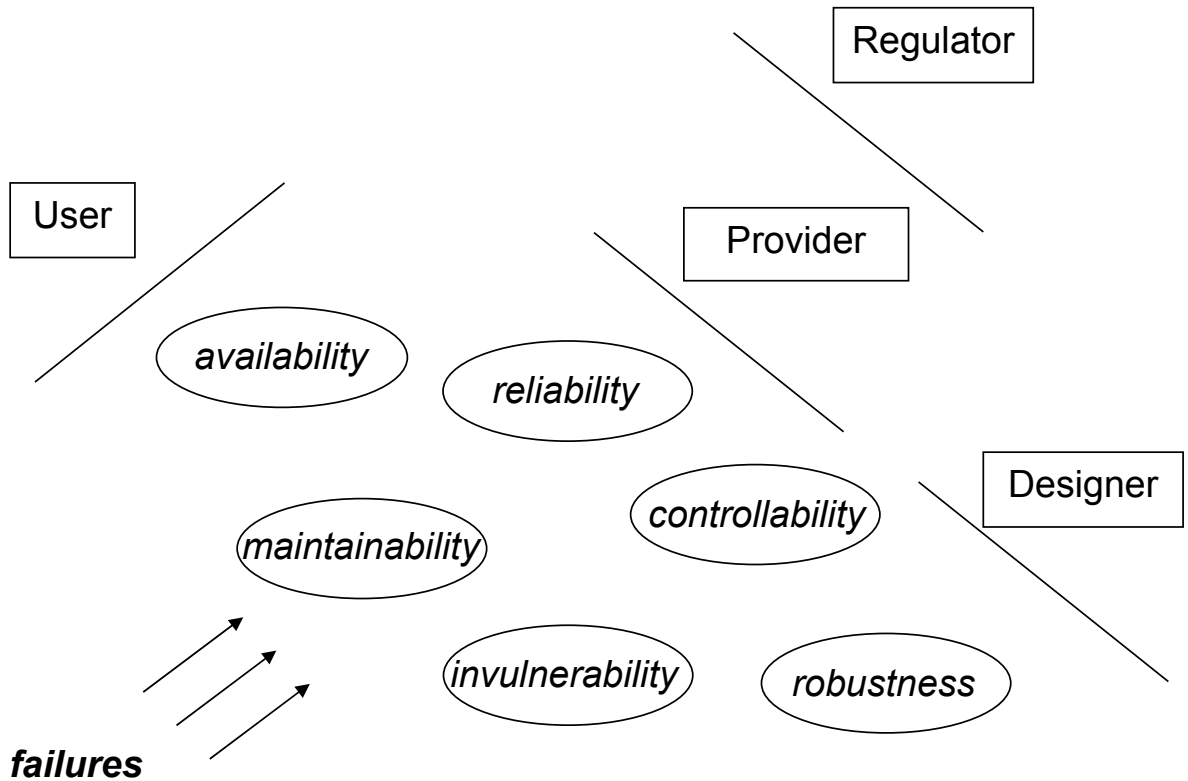
Pirkko Kuusela, Ilkka Norros, Urho Pulkkinen
VTT

Pekka Savola
CSC

Outline

- What is IP dependability?
- Dependability case methodology
- Case study: dependability of Funet's core network
- Discussion

Actors and aspects of IP dependability



Dependability case

- safety case $\longrightarrow$ 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

What is the purpose of Funet's dependability case

- Is dependability case the right way to address IP dependability?
- Is something more or different needed?
- *NOT* the final dependability judgement
- Keep in mind that this case is public
- Funet good network to work with
- Generality over speciality (breadth-first-approach), a meta-model

Elements of dependability case

GRAPHICAL VISUALIZATION together with

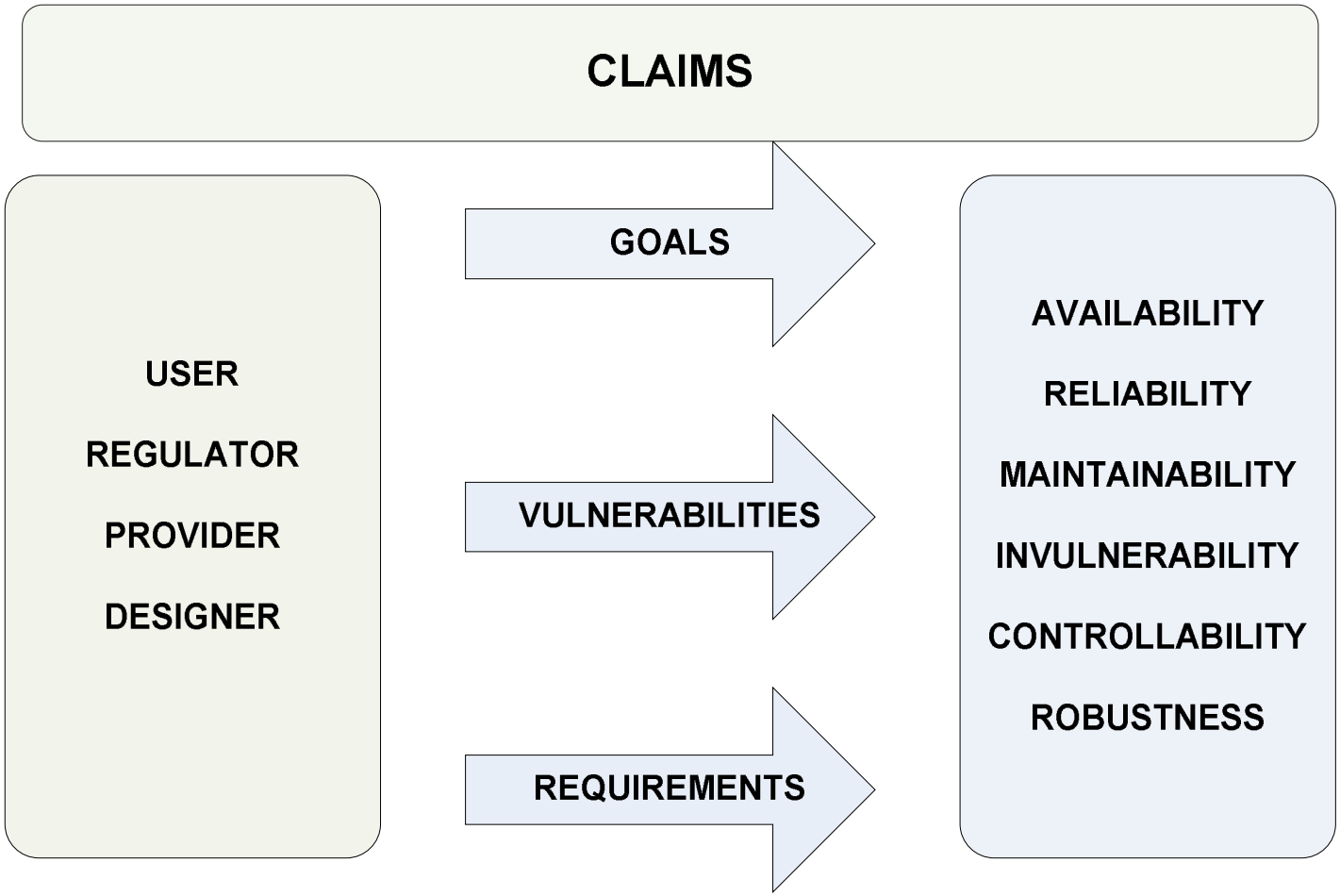
- *CLAIMS*
- *EVIDENCE*
- *ARGUMENTS*

Elements of dependability case

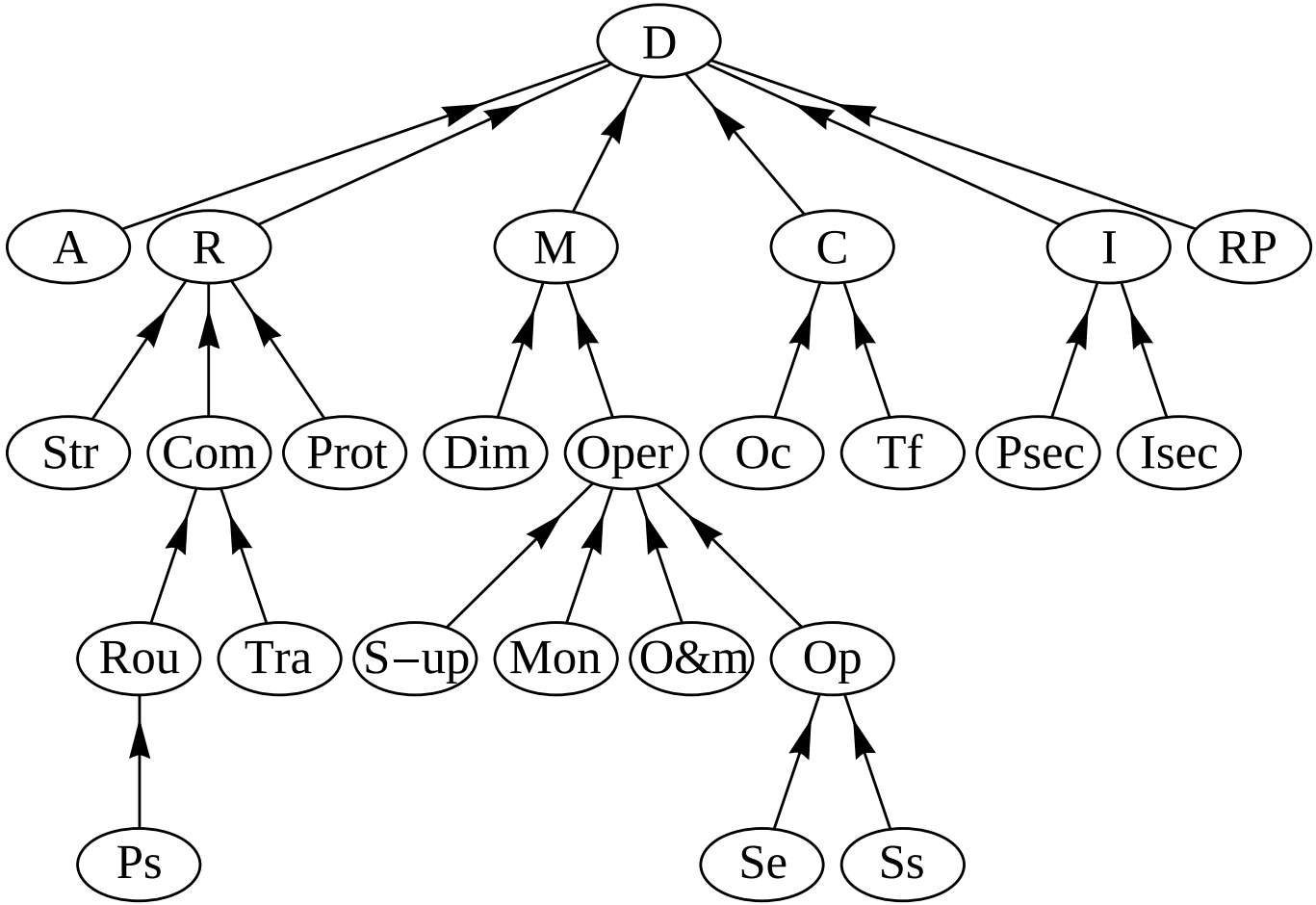
GRAPHICAL VISUALIZATION together with

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

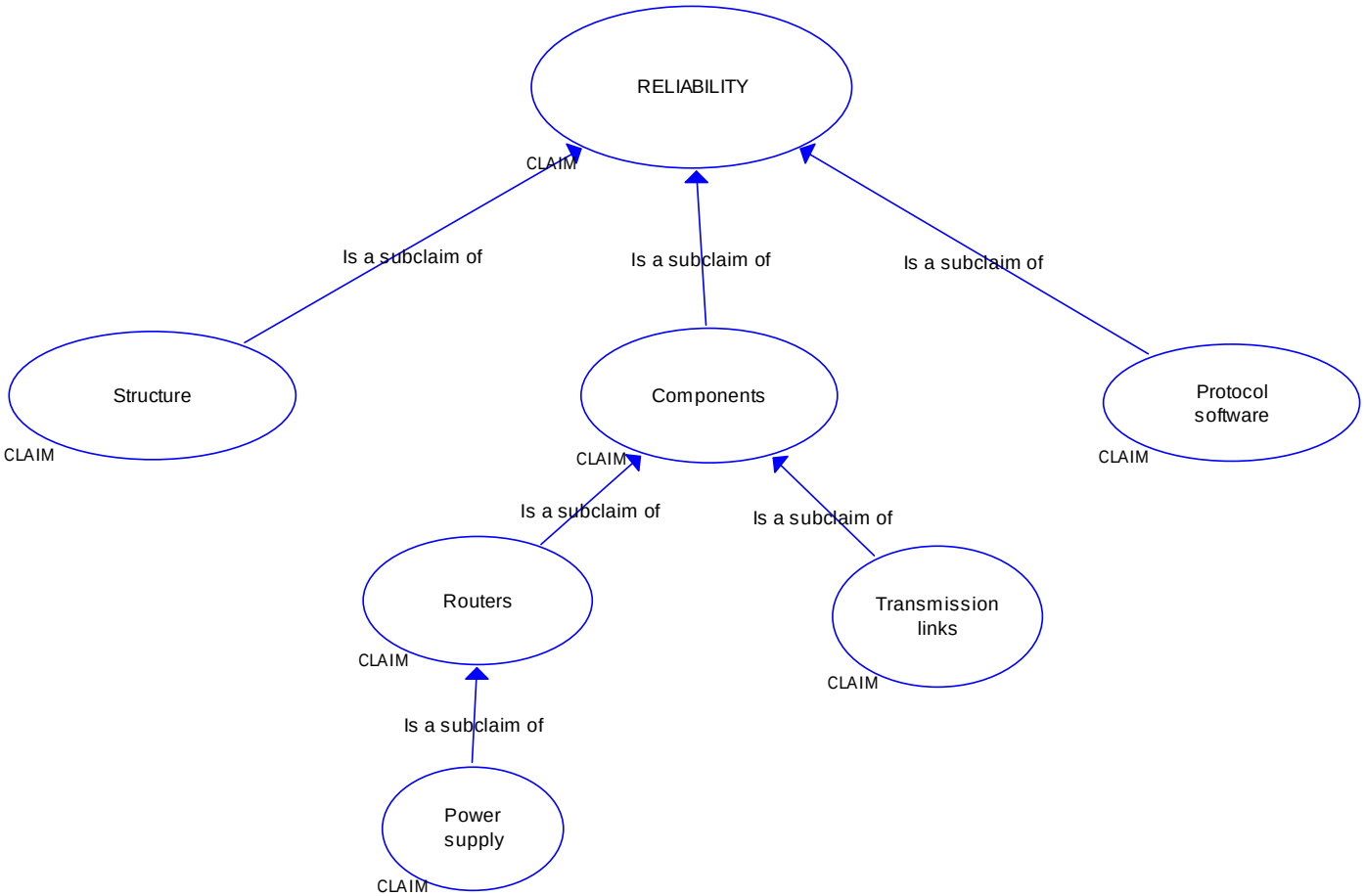
Where do claims come from?



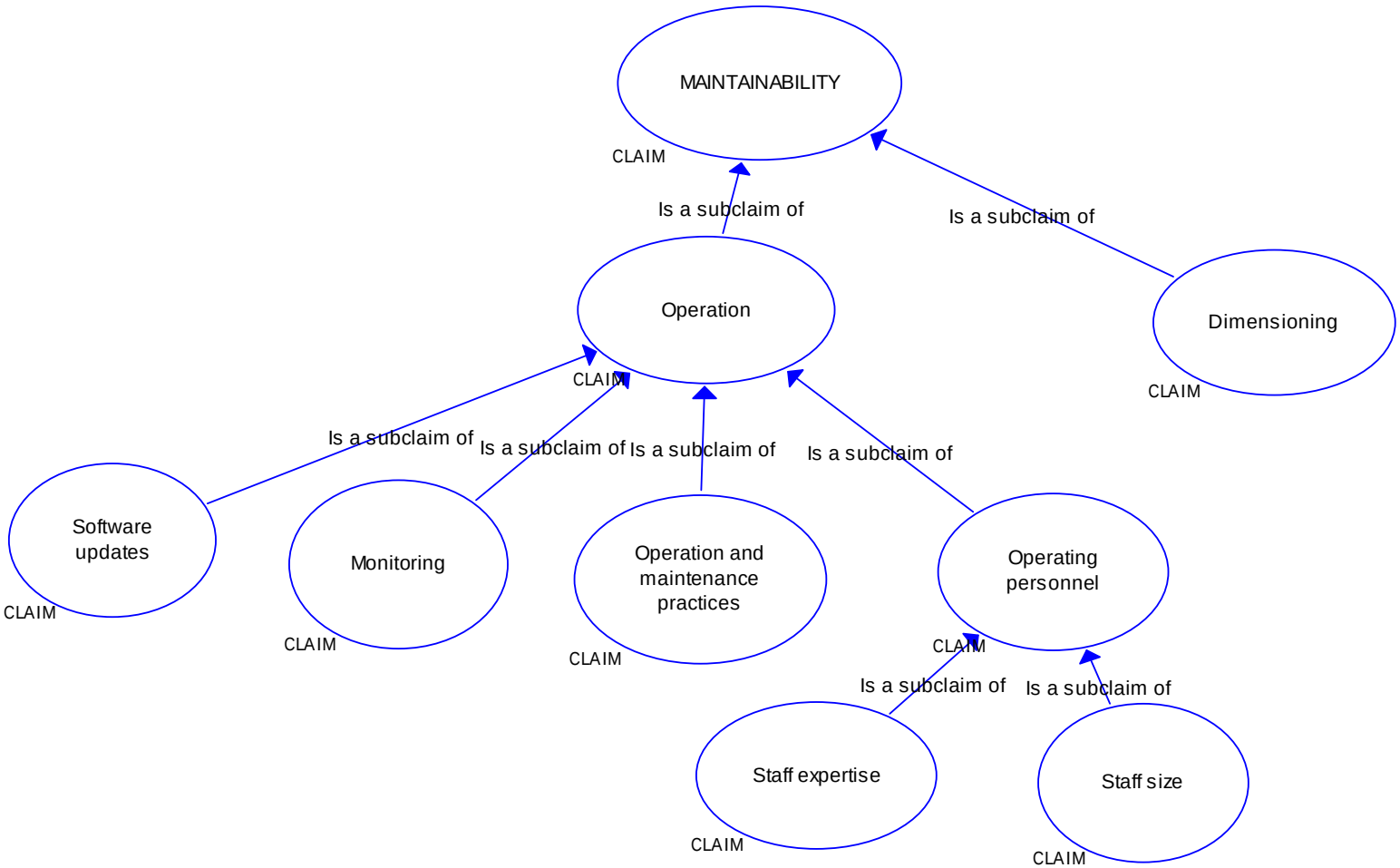
Claims


D
A
R
M
C
I
RP
Str
Com
Prot
Dim
Oper
Oc
Tf
Psec
Isec
Rou
Tra
S−up
Mon
O&m
Op
Ps
Se
Ss

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 ASCE and Claim-Argument-Evidence

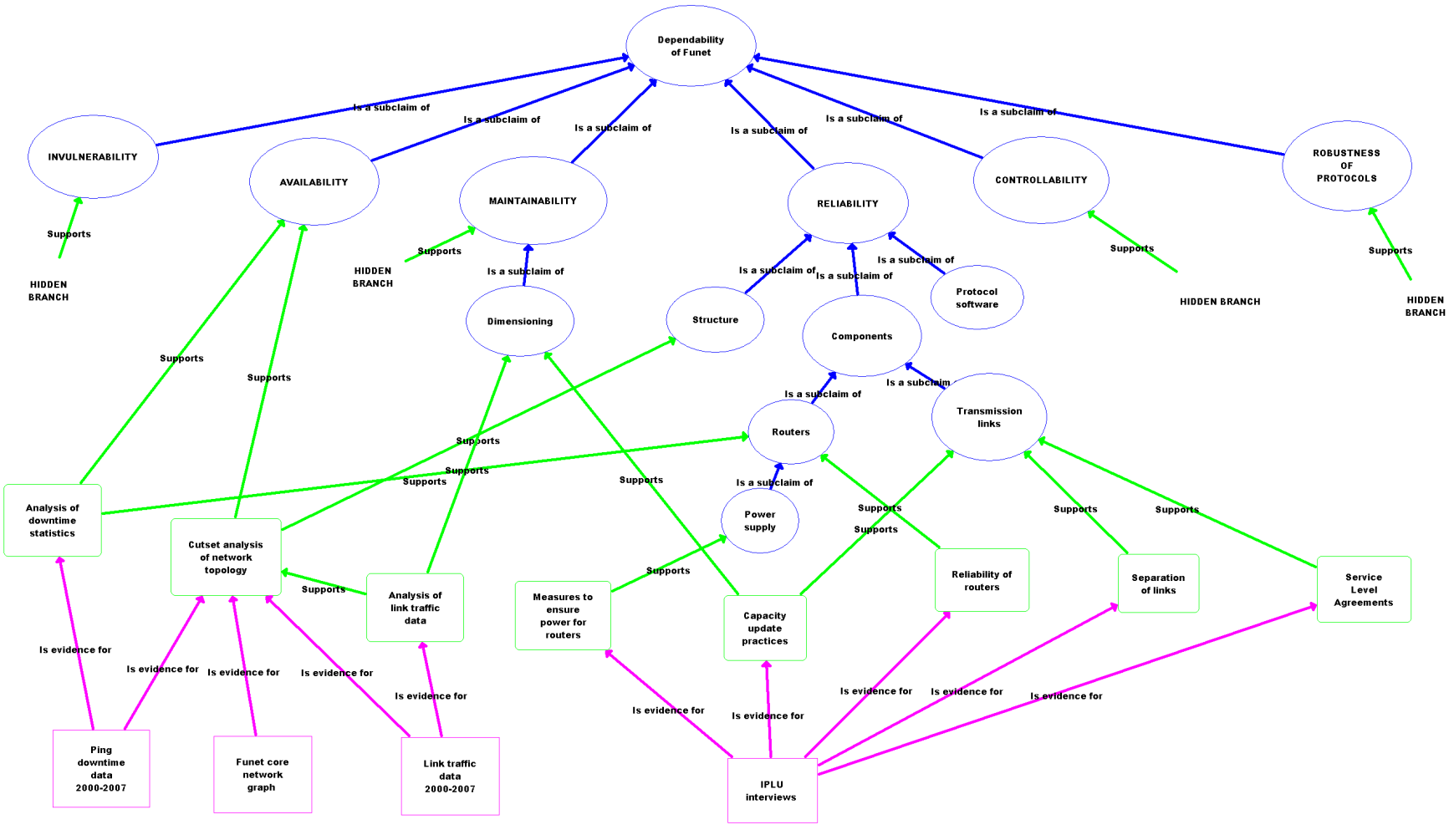
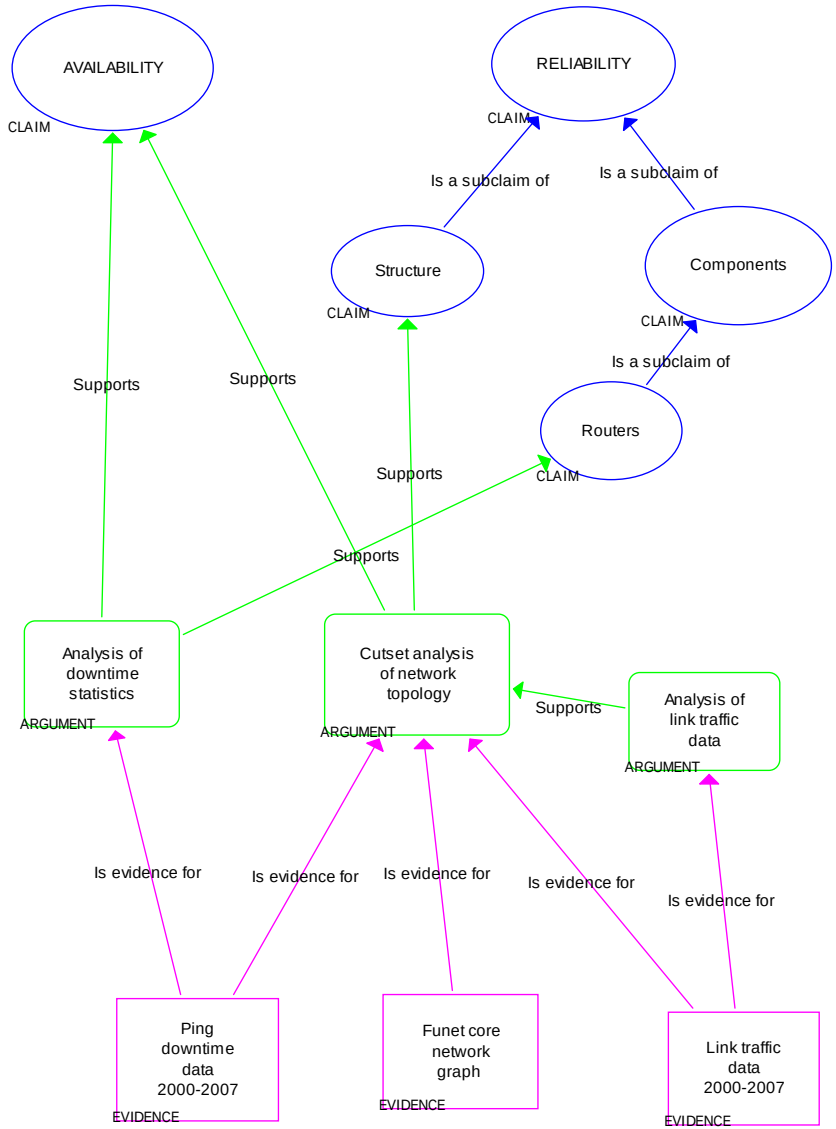
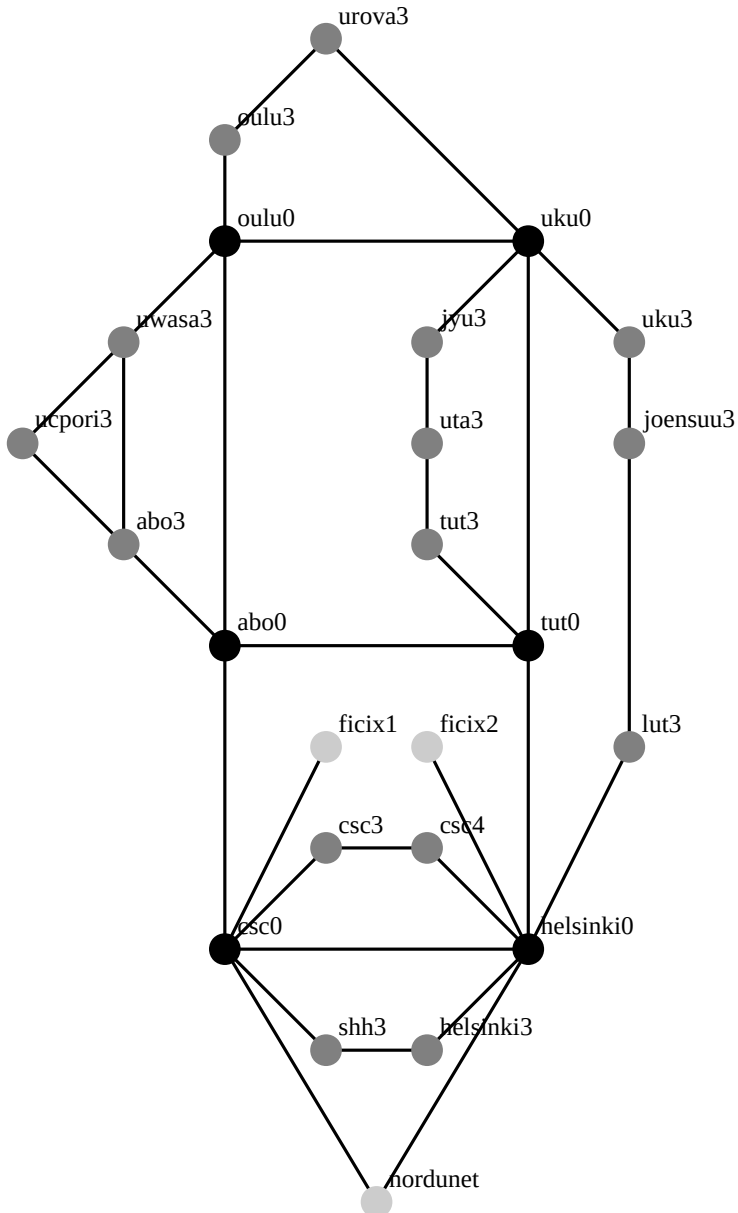


Illustration of ASCE and Claim-Argument-Evidence



Cutset Analysis

- topology (physical = logical)
- routing rules
- Funet OK if
  1. connected
  2. Ficix
  3. NorduNet



Cutset Analysis

theoretical failure cases, $\leq$ 3 links or nodes removed

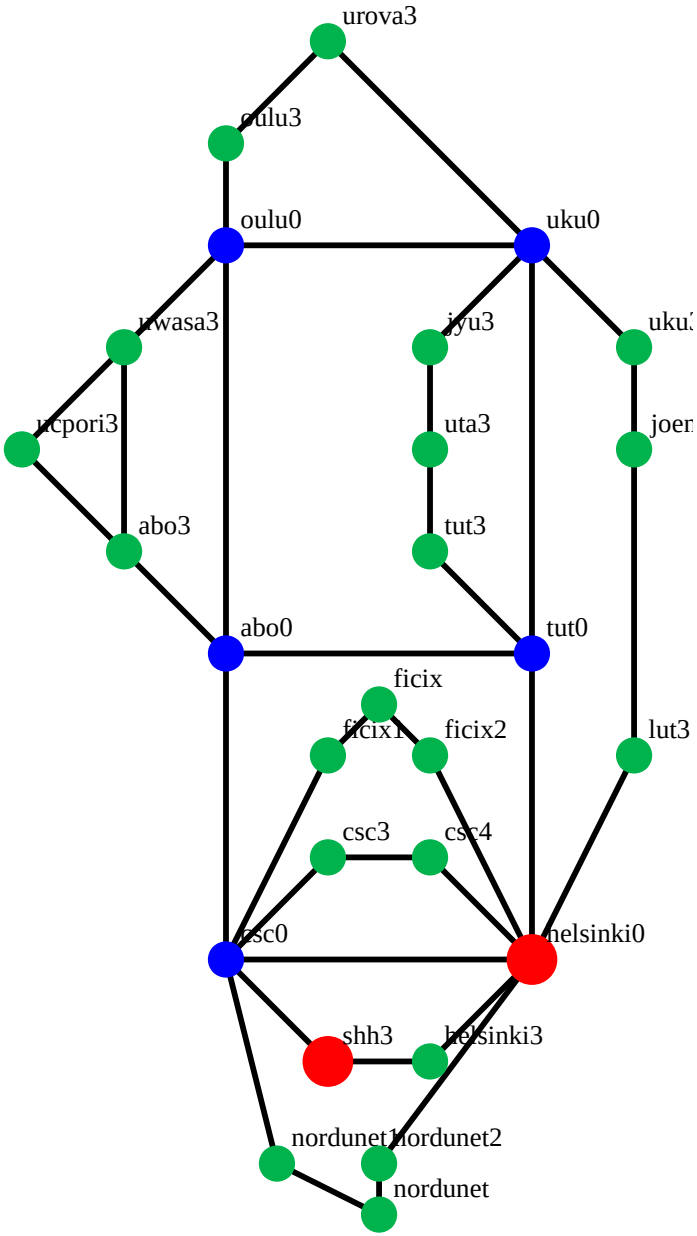
Failures:

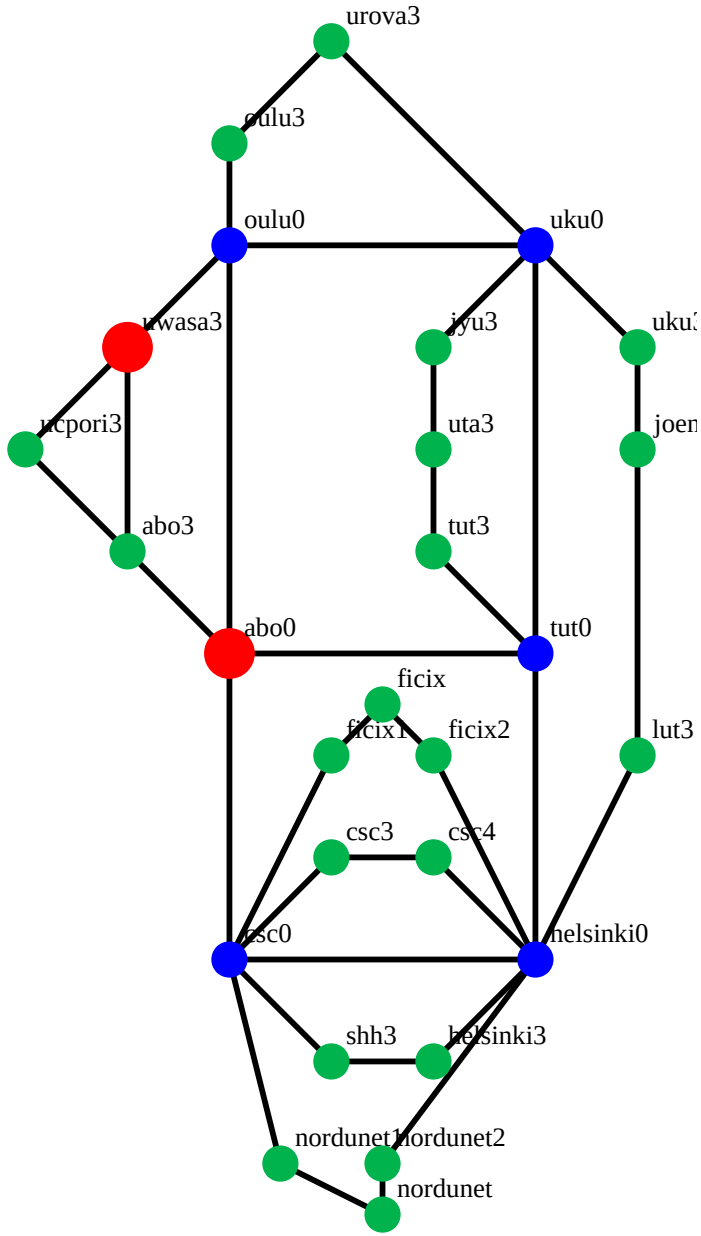
	type	how many
A:	0 links & 1-2 nodes	37
B:	1 link & 1-2 nodes	81
C:	2 links & 0-1 nodes	55
D:	3 links	13
	total	186

(3 nodes removed not included)

Cutset Analysis

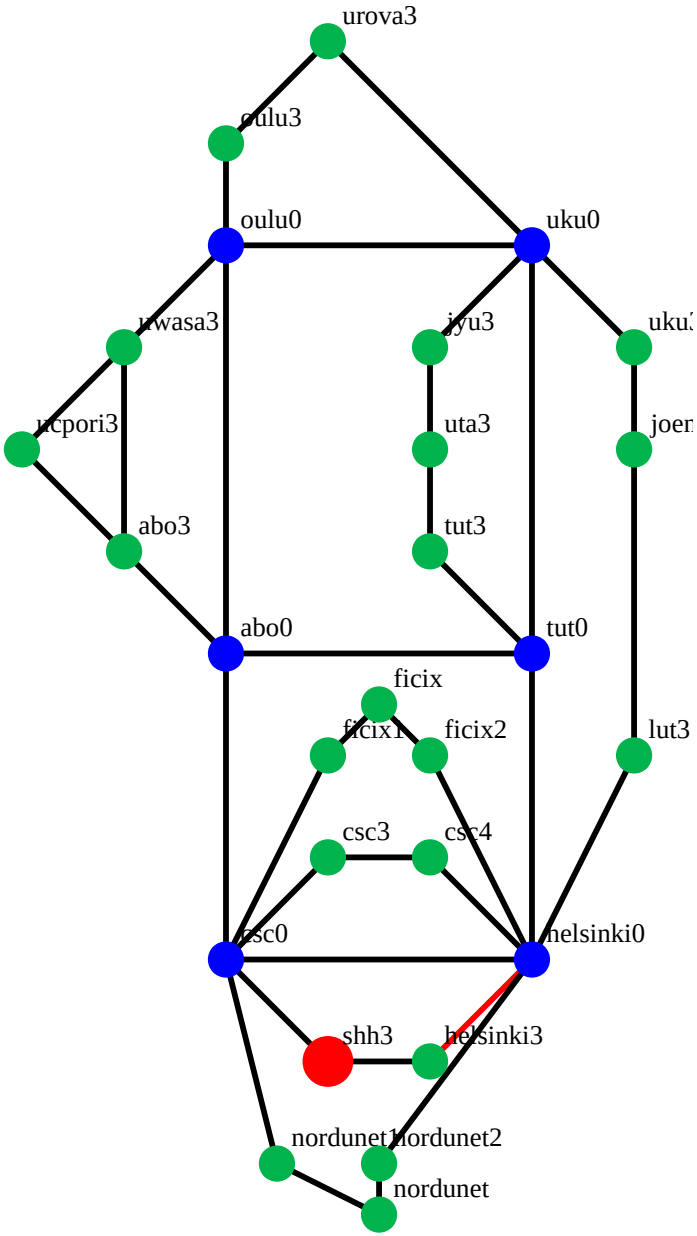
Failure type A: no links & 1-2 nodes, 37 cases

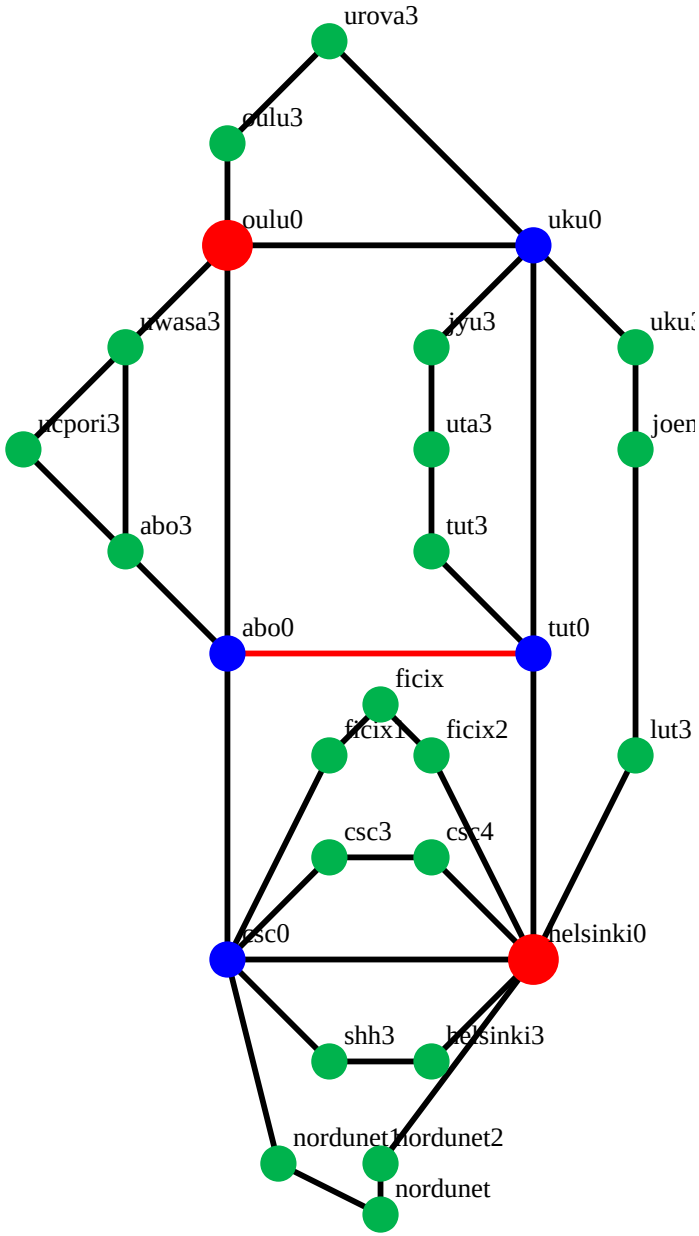




Cutset Analysis

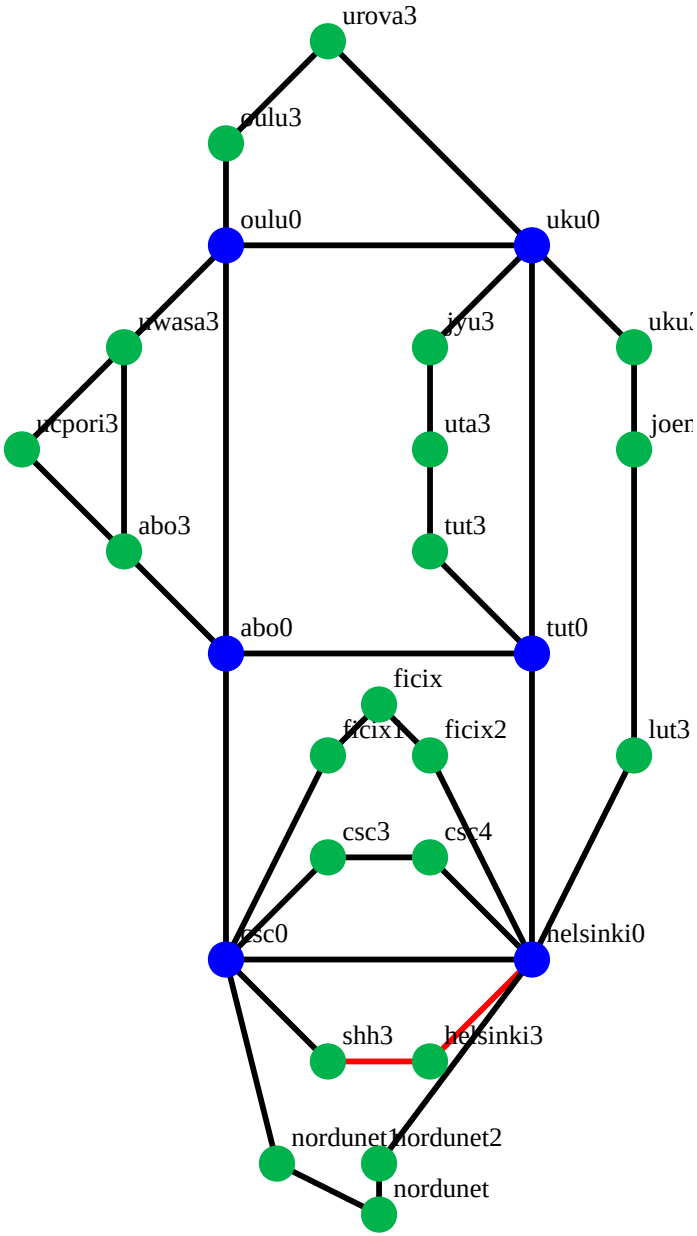
Failure type B: 1 link & 1-2 nodes, 81 cases

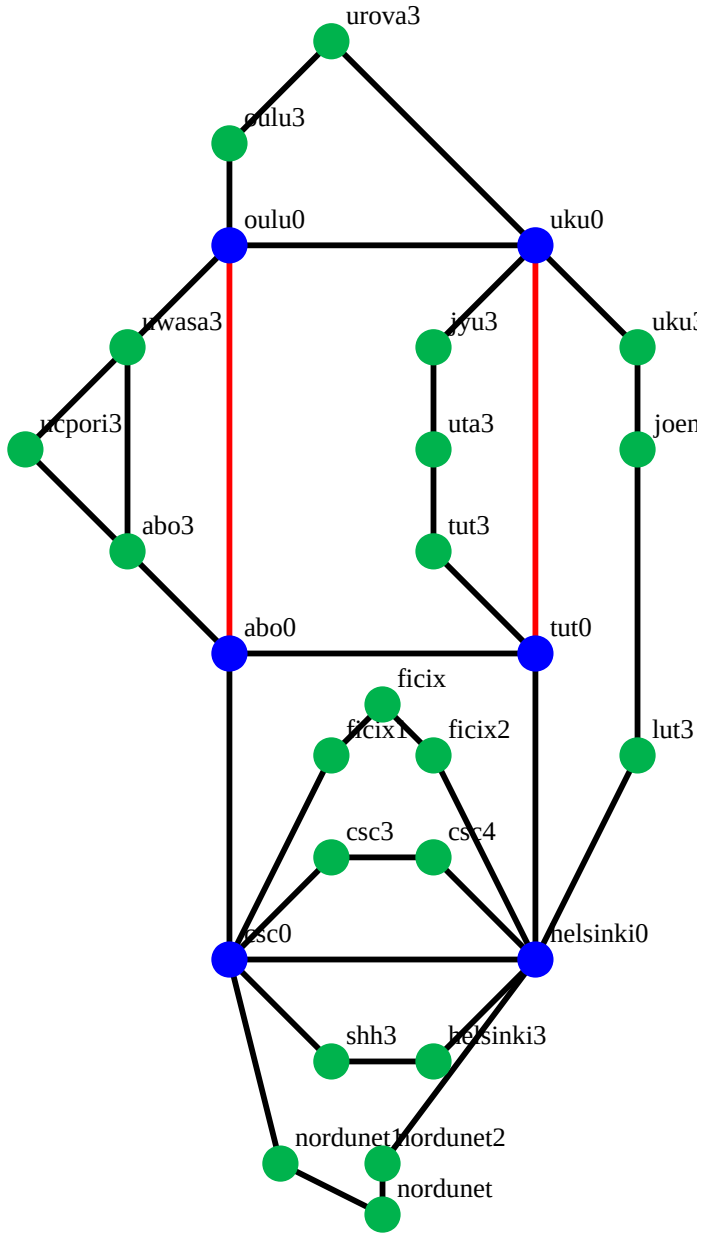




Cutset Analysis

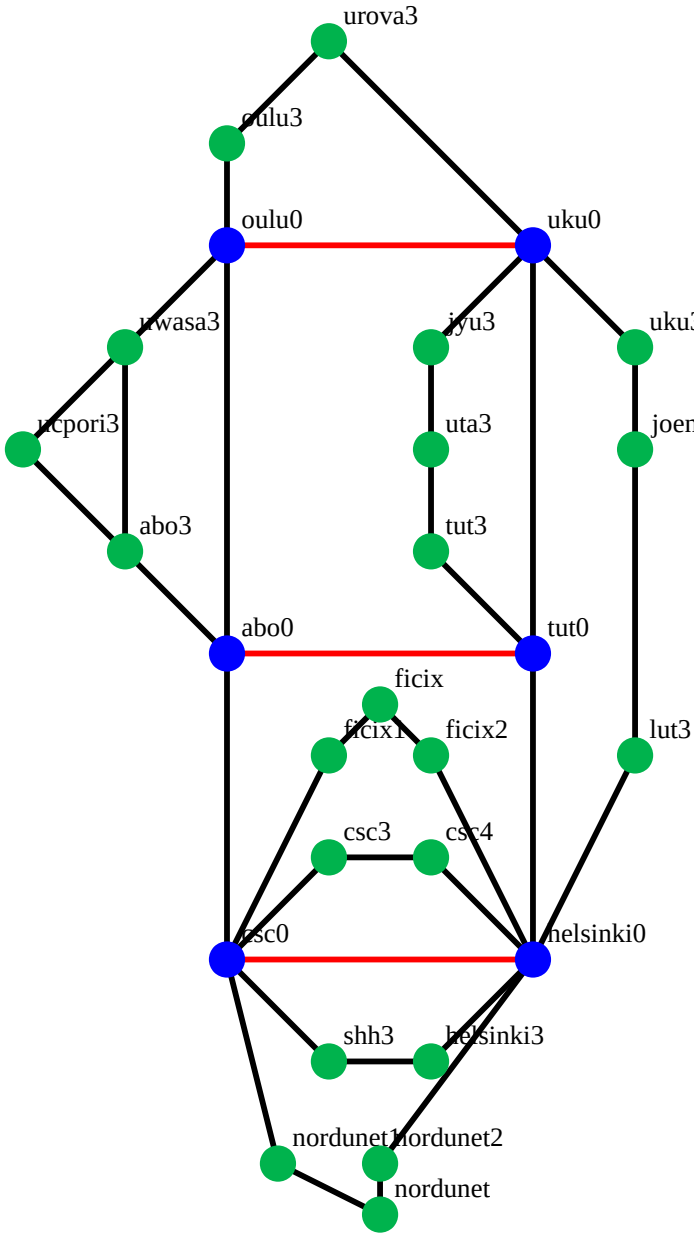
Failure type C: 2 links & 0-1 nodes, 55 cases

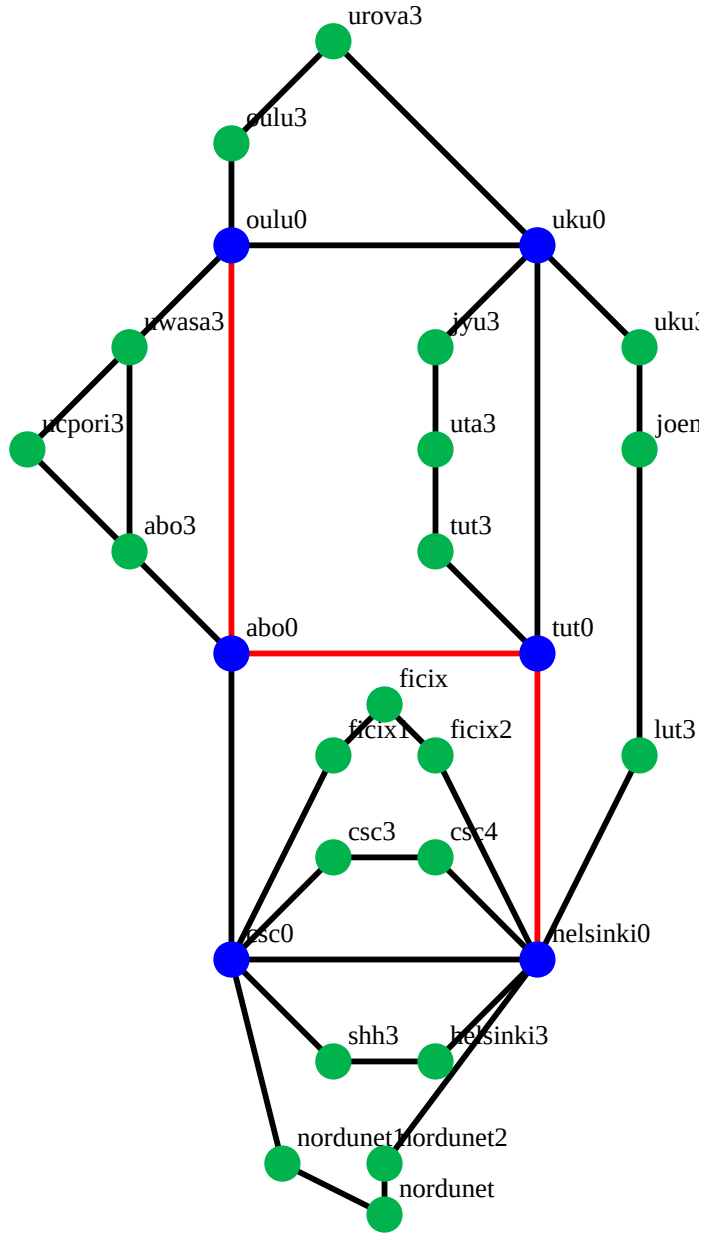




Cutset Analysis

Failure type D: 3 links, 13 cases





Cutset Analysis

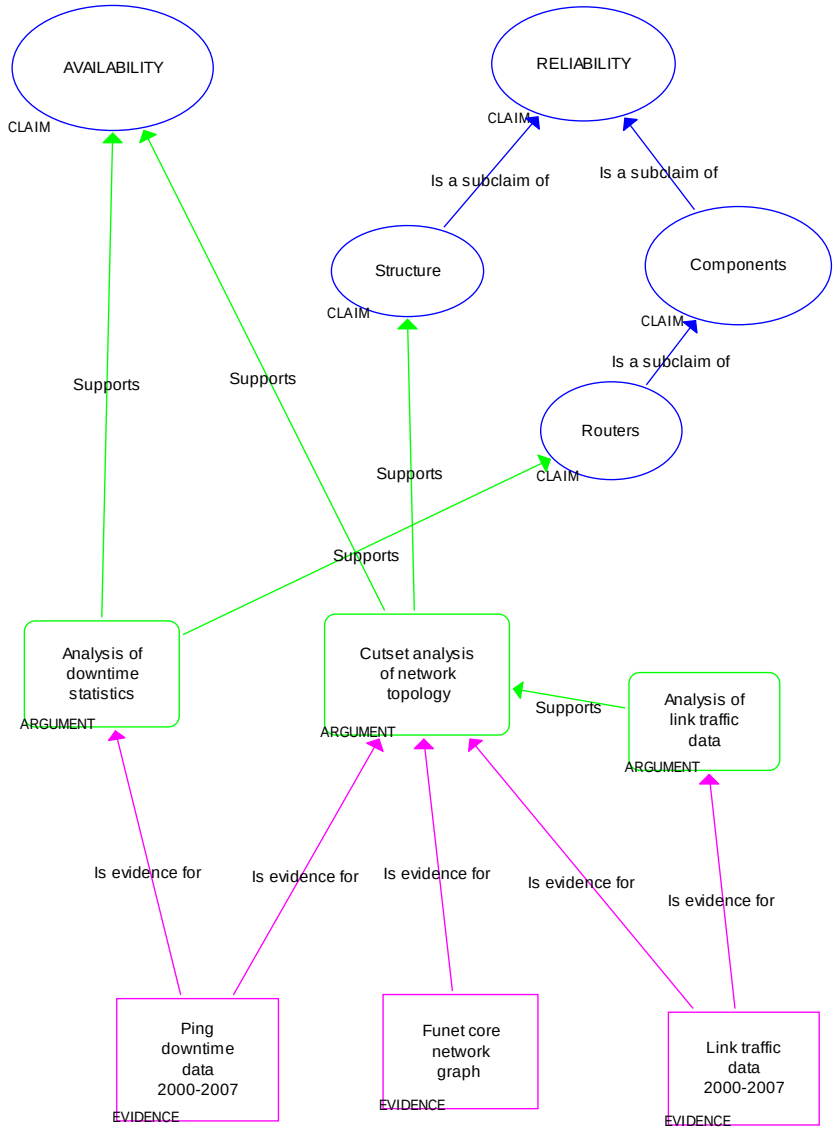
Can do more:

- 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??

Analysis of downtime statistics



Analysis of downtime statistics

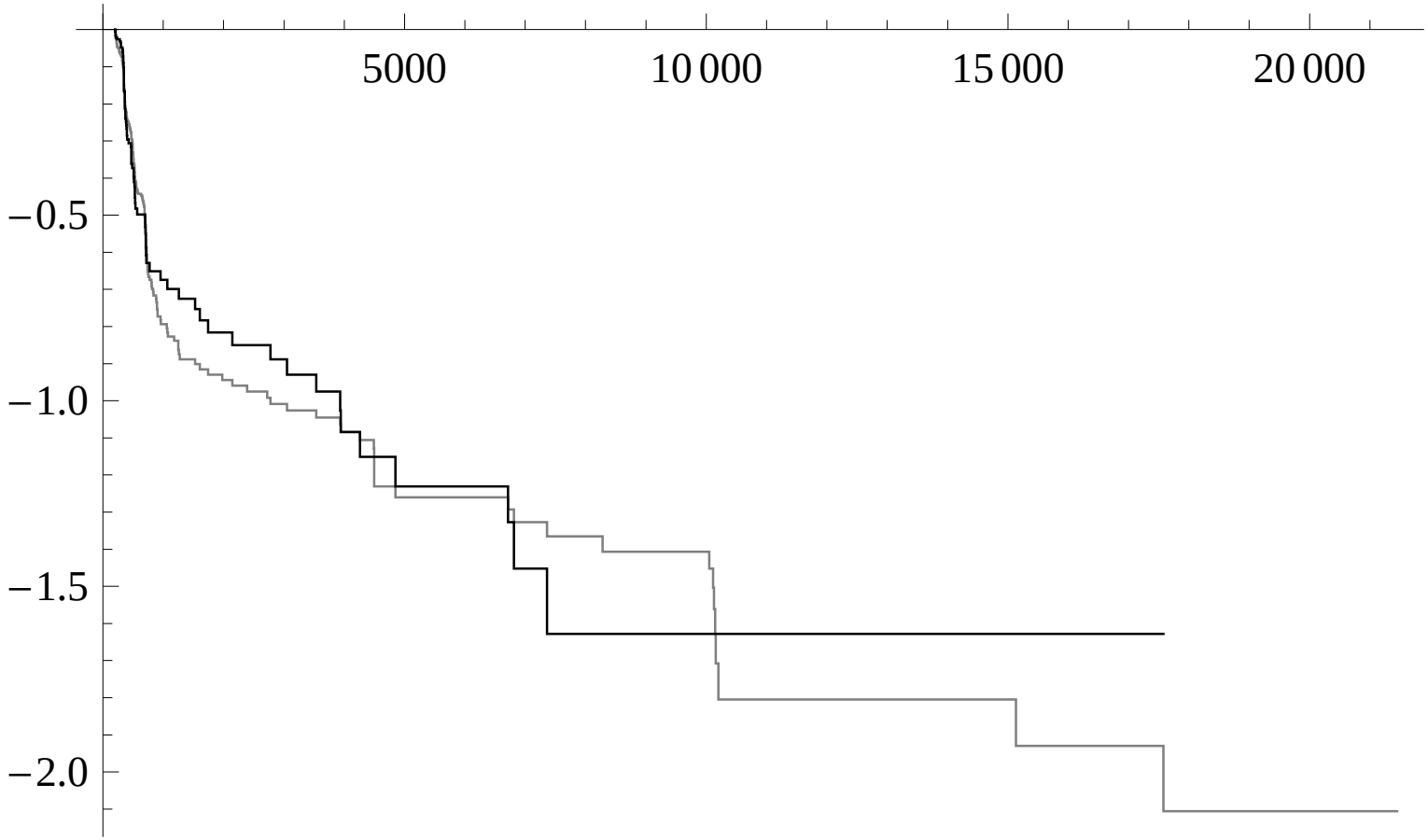
CSC ping data:

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

remark: individual downtimes $\neq$ independent rare events

Downtime analysis, core

Length distribution:

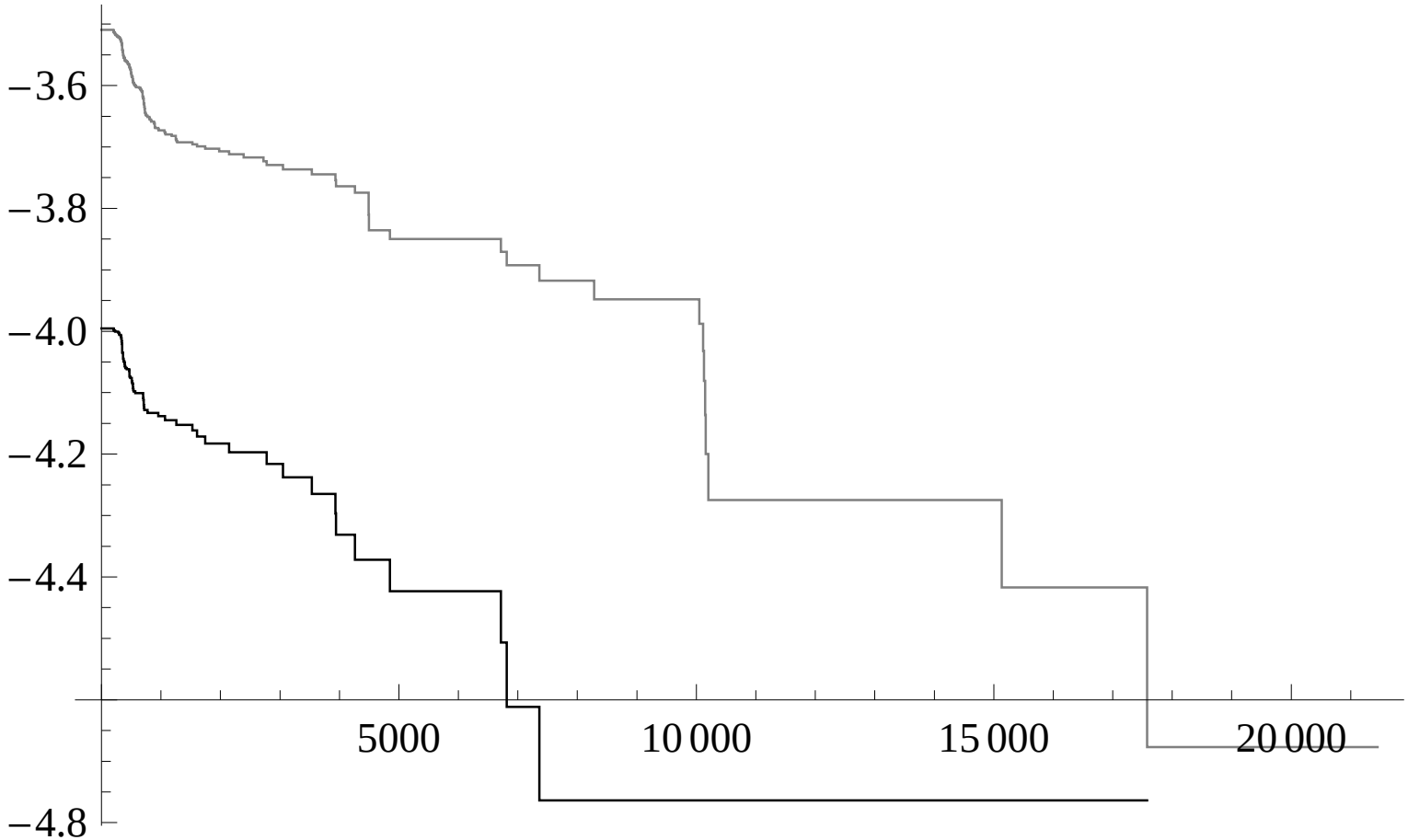


x = time in seconds

y = tail probability functions of downtime length distribution, $\log_{10}$ scale
all data in gray, clusters censored in black

Downtime analysis, core

Downtime frequency:



x = time interval length in seconds

y = downtime frequency curve, $\log_{10}$ scale, read 9's
all data in gray, clusters censored in black

Analysis of traffic

Wanted: link loads at most 50% of capacity, no single failure harms traffic

Tool for checking this:

- busy hour traffic values
- traffic matrix estimate (gravity principle)
- shortest path routes (using routing rules)
- Do: Remove links or nodes, reroute traffic, calculate lost traffic, check link loads.

supports: dimensioning & availability

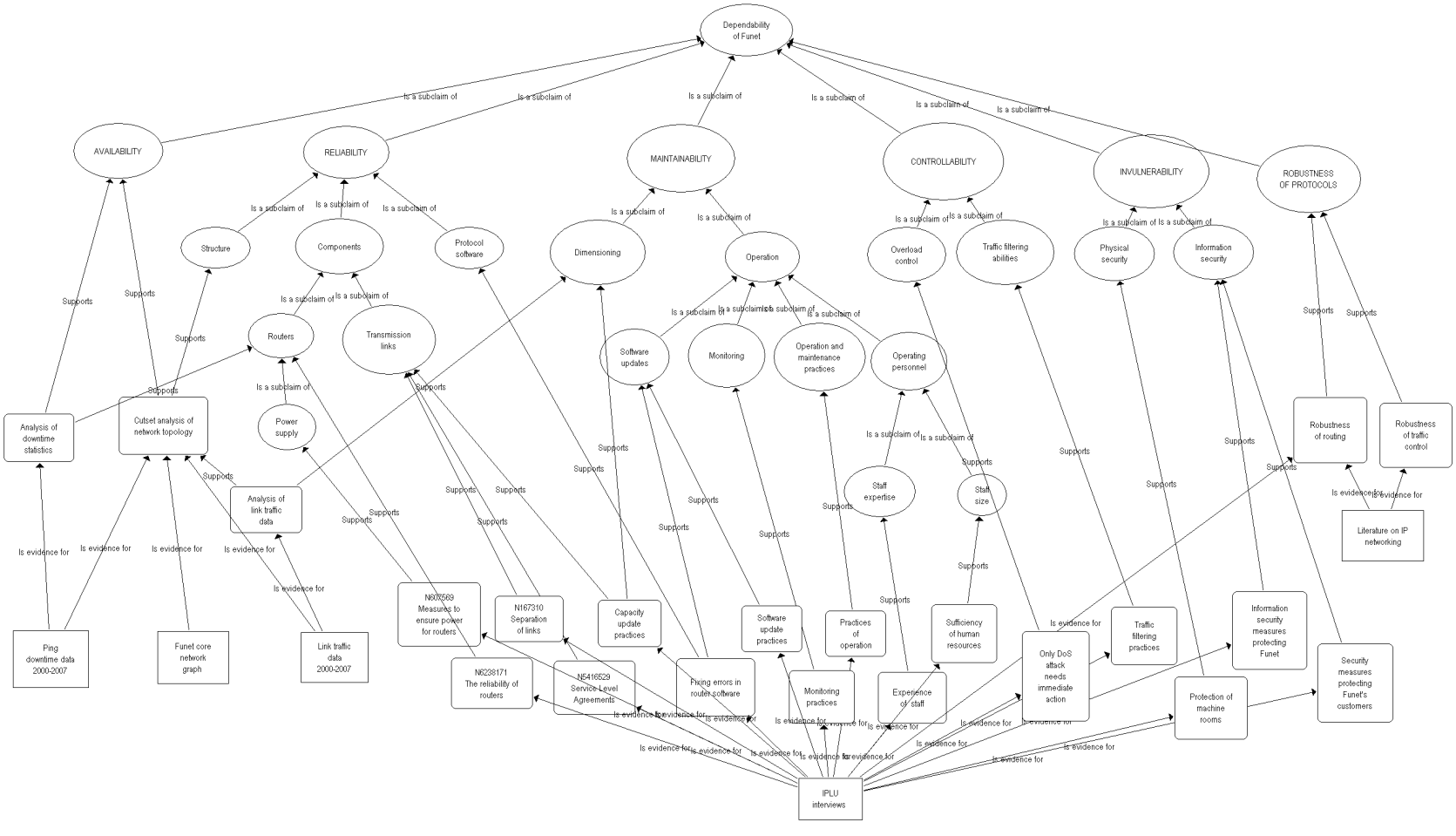
Qualitative argumentation

18 qualitative arguments

Some remarks:

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

Complete dependability case



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)