Towards Risk-aware Communications Networking

Ilkka Norros

VTT Technical Research Centre of Finland

Joint work with

Piotr Chołda	AGH University of Science and Technology, Kraków
Eirik L. Følstad	Norwegian University of Science and Technology, Trondheim
Bjarne E. Helvik	Norwegian University of Science and Technology, Trondheim
Pirkko Kuusela	VTT
Maurizio Naldi	University of Rome 3 “Tor Vergata”

Reference: P. Chołda, E.L. Følstad, B.E. Helvik, P. Kuusela, M. Naldi, I. Norros. Towards risk-aware communications networking. *Reliability Engineering and System Safety* **109**, 160–174, 2013.

Contents:

1. Background

2. Risk assessment

3. Risk response

4. Risk monitoring

5. Next steps

1. Background

Fact: we depend more and more deeply on a complex web of interdependent communications networks.

Risks associated to the failures of electronic communications reverberate directly across society.

We must be aware of those risks and decide how to face them.

Work in this area is dispersed in many regulatory, standardization, research, planning, operational and maintenance activities. When recognized and promoted as a whole, each part would really add to the meaning and significance of the others.

Following Kaplan & Garrick (1981), risk is the triplet of

- risk scenario
- likelihood of that scenario
- consequences of the scenario

Thus, we face a threefold task:

- clear recognition of *events* (and event sequences etc.) that challenge network dependability
- assessment of their *probability* (conditioned on available information, thus often subjective/Bayesian), taking into account *uncertainties* involved
- assessment of their *impact* (an element mostly neglected in our context so far)

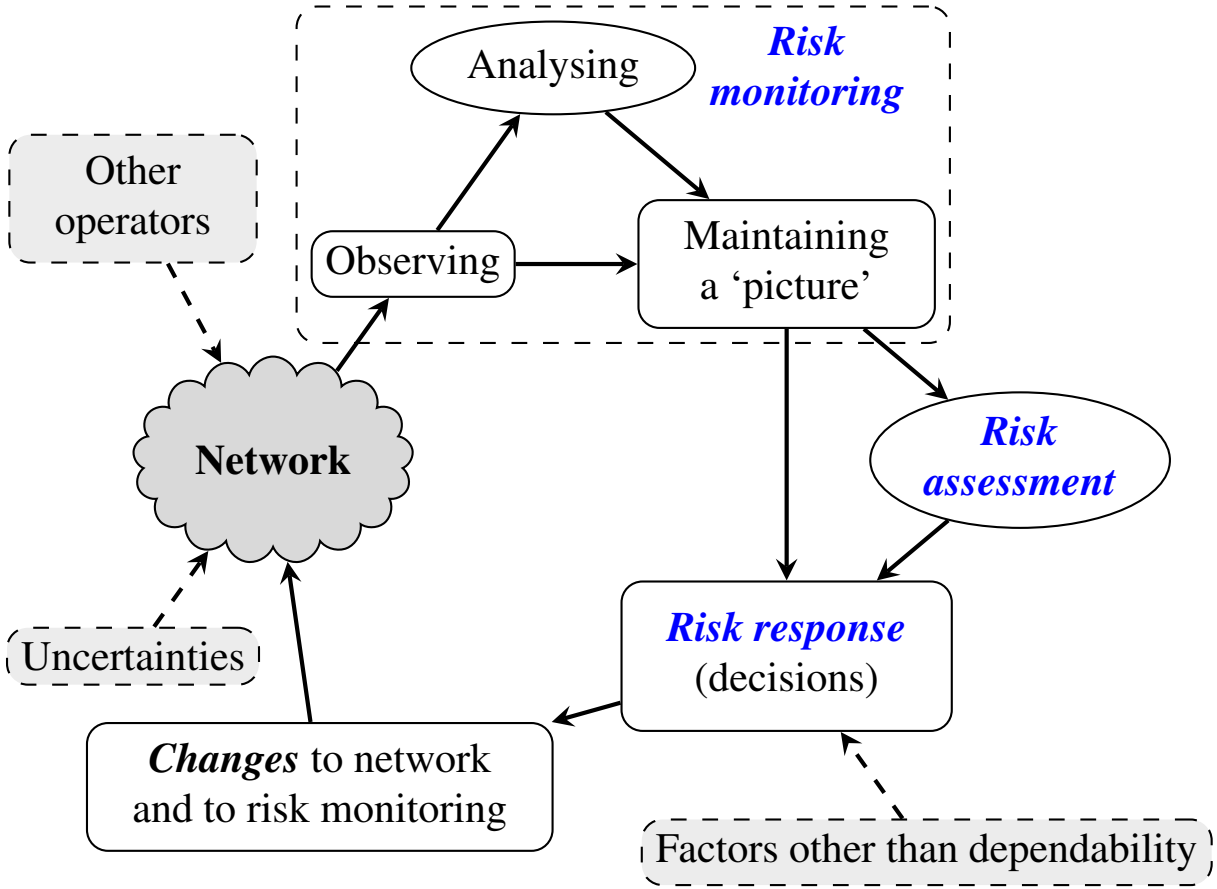
Structure adopted from NIST Special Publication 800-39 "Managing Information Security Risk":

- Risk framing: umbrella action producing the risk management strategy, where the following are accomplished:
- Risk assessment: identify possible problems and estimate their frequencies and impact
- Risk response: determine reactions to predicted risk; options: acceptance, avoidance, mitigation, sharing, transfer
- Risk monitoring: check how selected responses have performed and provide feedback to update response policies

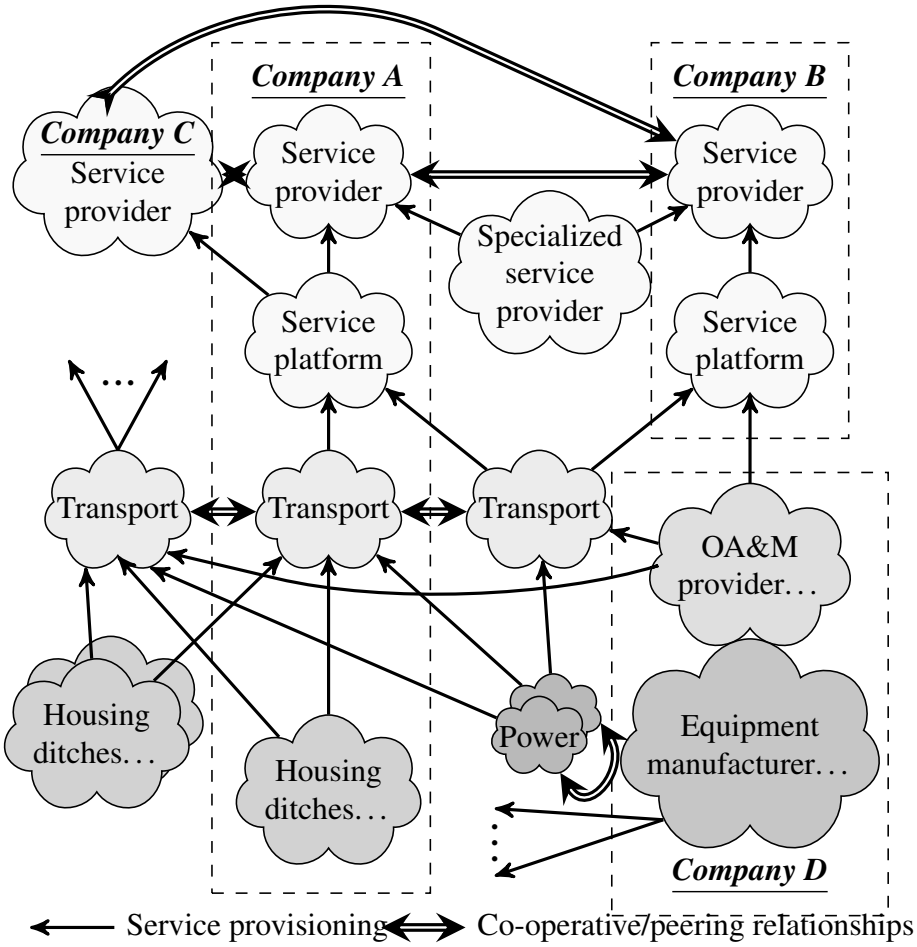
Actor classes and their characteristics relevant for network risk:

Actors	**Interests**	**Threats**	**Actions**
Providers	• Profit • Customer satisfaction	• Penalties • Loss of customers	• Care for dependability • Enterprise risk management
Users	• Availability • Quality and price	• Loss of connectivity or service • Business or life consequences	• SLA adjustment • Choice of a provider
Regulators	• Common benefit and societal needs • Competition	• Anarchy and monopoly • Breakdown of critical infrastructures	• Regulations • Collection of statistics
Researchers	• Innovative solutions • Understanding	• Lack of funding • Lack of focus	• Public promotion of ideas • Standardization

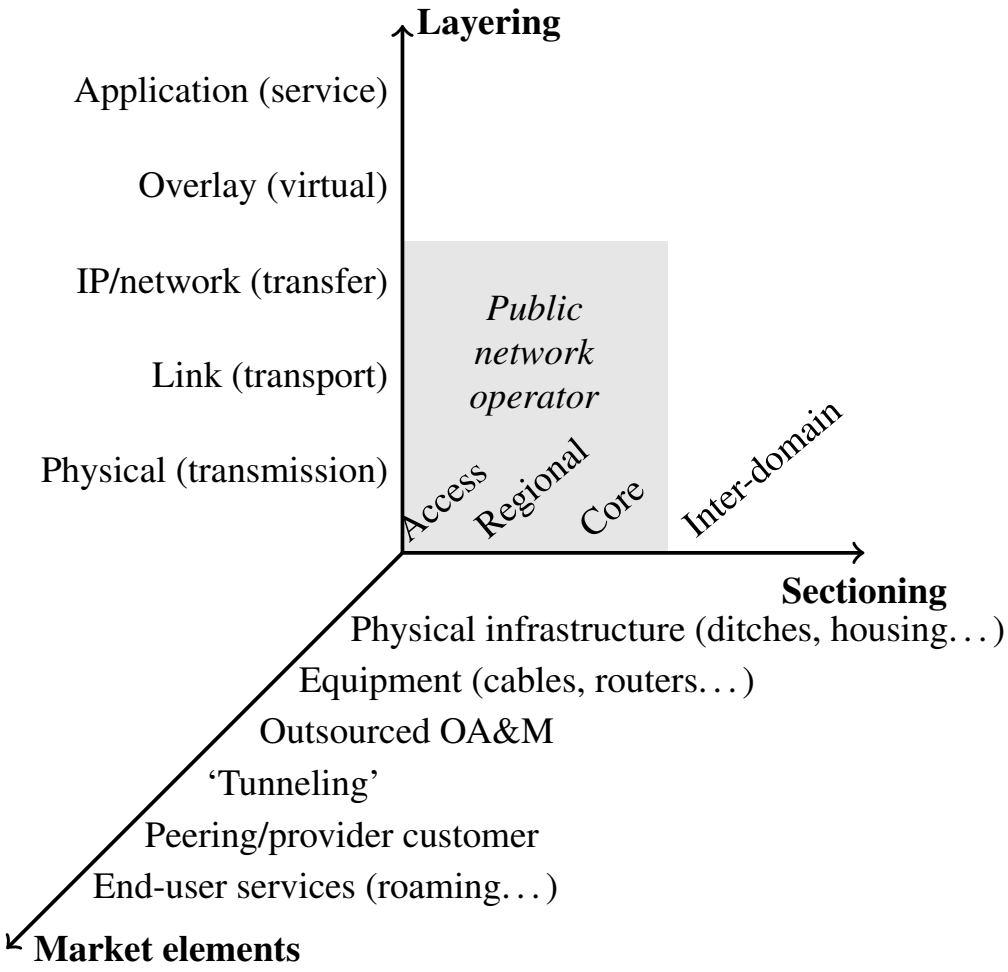
Provider's care-taking cycle of risk management:



"Big picture" of network service provisioning:



Dimensions of complexity:



Common complexity with aviation and railway systems:

- many competing providers sharing their resources
- business solutions are networked
- outsourcing is used
- continuous adaptation to new technologies

Major differences:

- communications networking does not have any central control unlike the ones used for common airspace
- availability is rarely sacrificed when problems arise
- incomparably fast, heterogeneous development of technologies, components, and network usage patterns (toy $\rightarrow$ alternative $\rightarrow$ dominant)

2. Risk assessment

We discuss the following questions:

- Network reliability assessment
- Estimation of service disruption impact
- Risk theory for networking

Network reliability assessment

- Failure statistics and modelling of failure processes
  - dependences between failure events:
    structural, dynamic, epistemic
  - non-Markovian character of failure processes

- Network reliability theory
  - how to compute network failure estimates from element failure statistics

Estimation of service disruption impact

A failure's impact for a service provider is determined by its multi-faceted consequences:

- lost traffic and revenues
- penalties by not meeting SLA
- indirect costs related to operator's reputation

In societal context, the impact of communication failures may be far larger than that suffered by the provider of the service, and all consequences cannot be measured by monetary terms.

In any case, the single most relevant element to enforce a risk-aware view by a network operator is SLA, where reliability, risk and costs are linked by agreed service features.

About risk theory

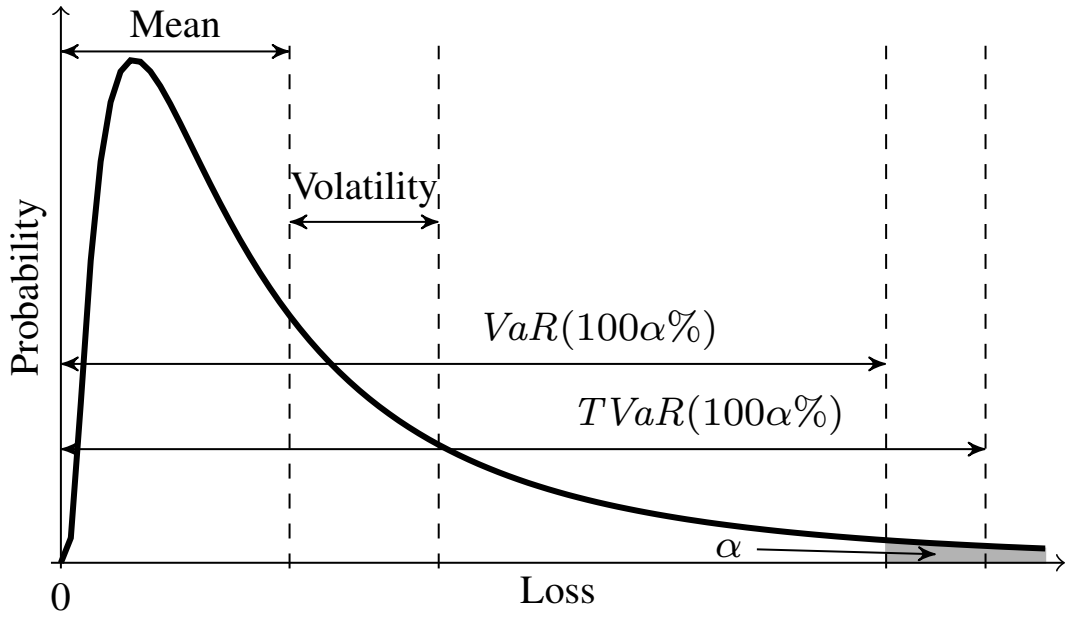
Mathematical risk theory is well developed in two contexts:

- Finance sector
  - aim: analyze variation of portfolio value as market conditions change; (i) market risk, (ii) credit risk
- Insurance sector
  - aims: (i) evaluate economical losses associated with an insurance policy; (ii) set insurance premium correspondingly
  - best known method for risk transfer!

In networking, we may consider a portfolio composed of customers and services and the losses associated with it.

Risk measures:

A *risk measure* is a functional $\rho(X)$ of the distribution of the random variable X presenting the loss:



- Value-at-Risk: $VaR(\alpha) = F_X^{-1}(\alpha)$
- Tail Value-at-Risk: $TVaR(\alpha) = \mathbb{E}[X|X \geq VaR(\alpha)]$
- multivariate risk measures

A major difference:

- finance and insurance: events of interest are point events (default of a company, the disaster occurrence)
- networking: most events of interest have an associated duration, and losses grow with duration of the event

Challenge of correlated variables:

- failures are often correlated or depend on a common source of failures
- even if failures are uncorrelated, risks associated to SLAs are correlated when they refer to same network region

3. Risk response

We divide approaches to risk response into two groups:

- Technical means
  - design the network to apply survivability mechanisms
  - new option: use differentiated mechanisms to address many levels of risks related to various types of services
- Market means
  - potential quick win option for an operator lacking resources to effectively use technical means or using additional methods to protect its value chain

Recovery methods and service differentiation

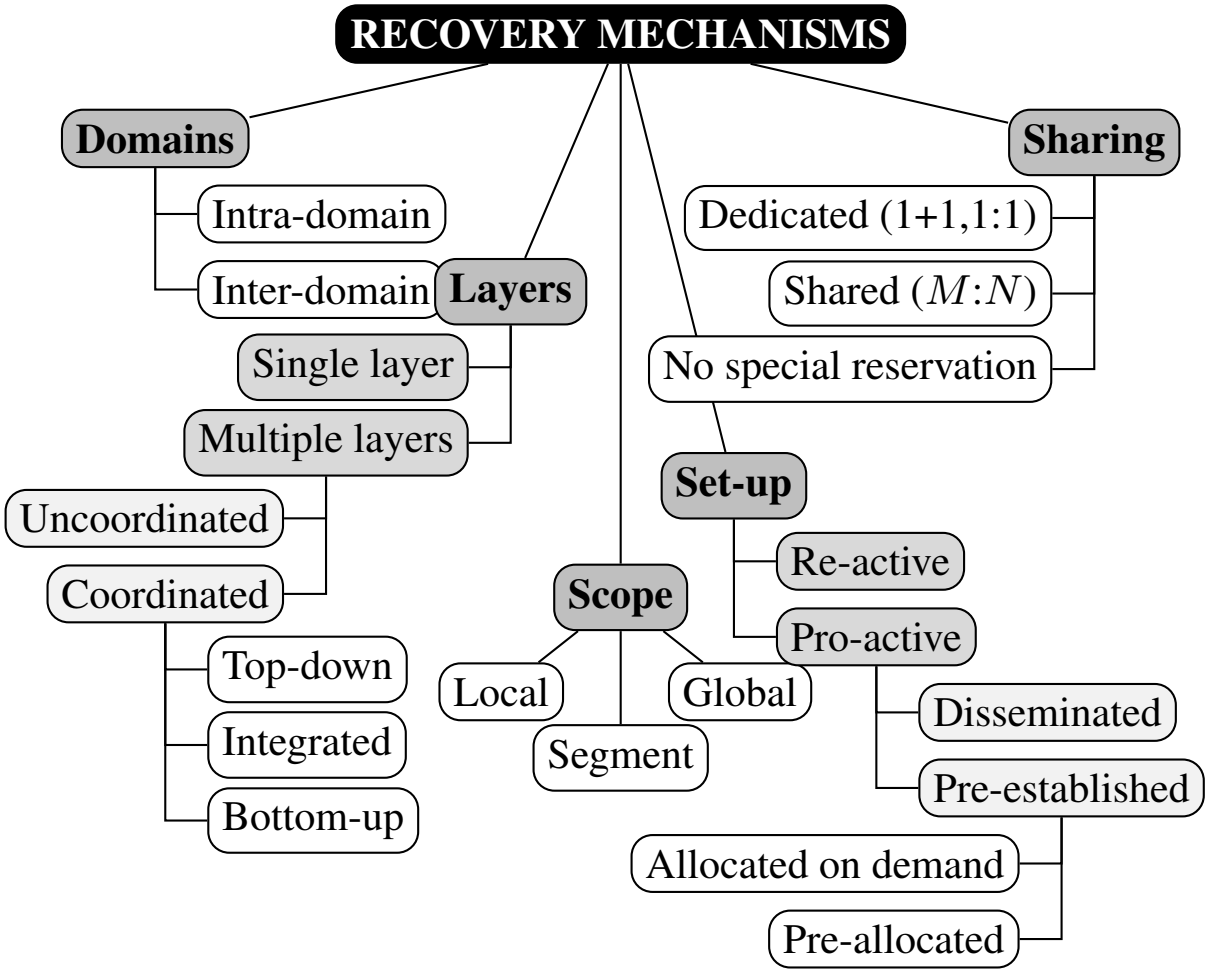
Risks can be mitigated by making networks resilient through automatic recovery mechanisms.

Two approaches to network resilience:

- *engineering* approach: reduce disruption using technically available mechanisms; choice of network technology limits the set of available recovery methods; bottom-up
- *operations research* approach: minimize costs assuming some constraints (e.g. on quality) and selecting optimized recovery method from a broad spectrum of possibilities; top-down

Recovery mechanisms can also be applied to introduce service differentiation — a form of *risk sharing*, since customer and network operator may use SLA to agree on levels of responsibility.

Classification of recovery mechanisms:



Market means

A risk management approach to network dependability considers risk mitigation and hedging strategies as accompanying the network-related ones.

Classification of management level protection measures:

- *expansive strategies*: aim to preserve revenue stream
  - keep service going relying on networks of other operators
- *protective strategies*: aim to recover damage due to failures
  - accept loss resulting from failure, but recover at least part by subscribing to insurance policy

Alternative forms of financial protection:

Insurance:

- operator pays a premium against network disasters
- operator receives compensation on their occurrence
- e.g. strategy against security risks Internet, proposed by Jean Bolot

CAT (catastrophe) bonds:

- operator issues a bond, which is bought by investors wishing to take on the risk
- operator pays a periodic coupon
- if the event that is insured against takes place before the bond's expiry, the operator is not obliged to pay the principal back

4. Risk monitoring and related practices

Issues discussed in the whitepaper:

- relationships of Internet market players and the role of regulators in this market
- practical aspects of network operation, including human factors
- practices and challenges in collecting and using data for active risk monitoring

Networking marketplace and regulators

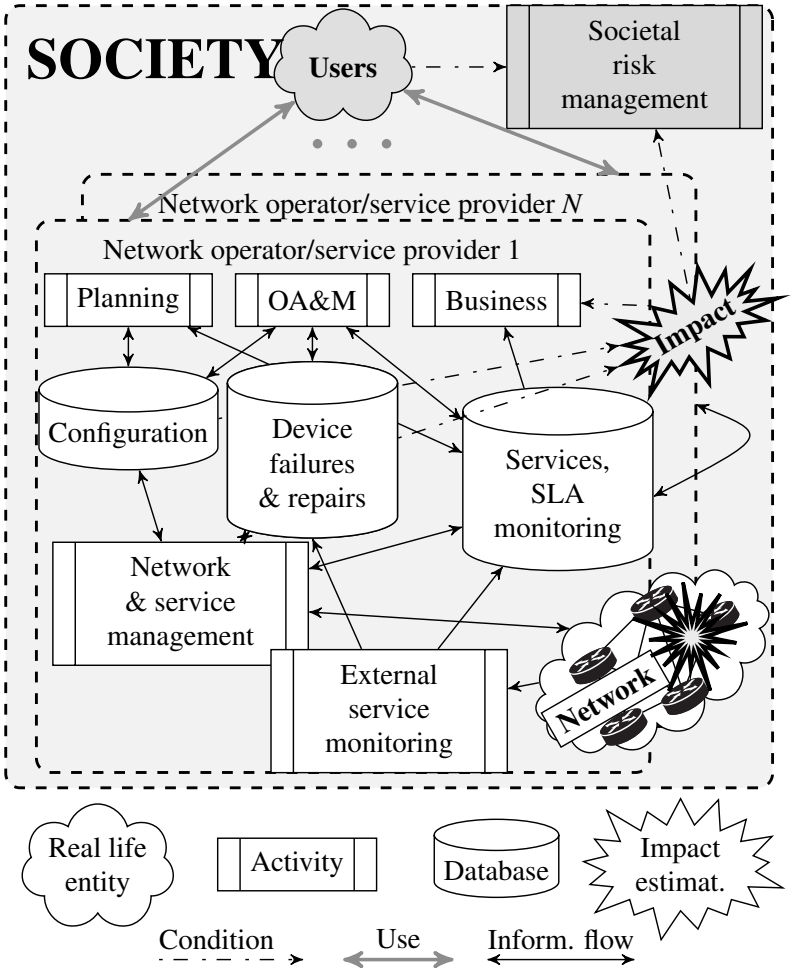
Examples of regulators' activities to ensure availability of affordable, good quality and future-oriented services:

- EU Directive on universal service at European level
- body of telecommunications regulations defined by the FCC (Federal Communications Commission) in US

Regulators' requirements have significant impact on the networking ecosystem, thereby on risks associated with the services.

Thus, enabling adequate risk assessment and management should be one of the aims.

Network risk related data flow:



Data collection for risk monitoring

Operators collect huge amounts of dependability-related data. However,

- the collection is aimed neither at reliability prediction nor at risk monitoring and assessment
- rather, these data are used for network and service provisioning, management, and OA&M tasks
- there is no common approach in failure data collection among network operators and service providers
- these data are not available for research in public domain

Addressing risks in societal context requires information to be available outside the market actors that own them:

- network structure
- operational and commercial cooperation among providers
- operational statistics

Current practice keeps most of this information confidential.

A firm and decisive approach from national and international bodies is required to control networking risks.

This must be followed by standardization bodies in defining which information shall be disseminated, how, and in which format.

Failure event data collection

Using collected failure event data for risk monitoring is still hard. Lot of information is needed to analyze correlations between failures:

- network topology
- traffic handling mechanisms
- recovery mechanisms

Such information is fragmented among different systems.

Moreover, data from different market actors should often be considered jointly.

A minimal *failure event record* contains

- equipment identifier
- start time of failure
- repair time of failure

However,

- event data must be put into *context*, and context stored
- *meta-data* needed for correct interpretation of fault data is seldom stored comprehensively
- *incident information*, such as classification, root cause identification or priority, need to be linked to failure events

5. Goals and next steps:

Overall objective				Intermediary steps
Objective	**Features, indicator(s)**	**Baseline**	**Target**	
Design, planning & assessment taking into account risk-awareness	Assumed level of risk	Qualitative treatment of risk at best	Risk (event-frequency-impact) in a goal function	Extension of a set of parameters involved in network design and SLA construction, risk as a constraint
Proper risk assessment	Used reliability metrics	Availability as an implicit measure of risk/loss (in the services context)	A set of explicit measures of risk (frequency of events and their severity, along with the assessment of their uncertainty)	Definition of the relation between network reliability and risk assessment
		Mainly connectivity assessment	Quantification of the network ability to provide services with required QoS levels	Inclusion of QoS/QoE measures in reliability assessment
		Loss measured at the traffic level	Loss assessed at the service level	Development of proper loss models taking into account layering and indirect impact
	Used risk metrics	Risk expressed implicitly as selected reliability metrics	Rich set of explicit risk metrics actively applied and induced by business and societal conditions	Definition of adequate risk measures for communications networking
Risk-aware data collection	Analysis-friendly collection of failure data	Detailed failure data utilized almost only re-actively, for repair purposes	Analysis of failure data as a continuous activity; results are used in risk assessment and network design	Working on existing data to improve monitoring and to reveal improper assumptions related to risk assessment
	Modeling of dependen-cies	Basing on the independence assumption	Correlations between failures taken into consideration	Collection of more detailed data