Risk-Aware Design and Management of Resilient Networks

(Keynote)

Piotr Chołda
AGH University of Science and Technology
Department of Telecommunications
Kraków, Poland
Email: piotr.cholda@agh.edu.pl

***Abstract*—The keynote presents a current view on the design of networks resilient to non-malicious failures supported by risk engineering.**

***Keywords*-continuity; optimization; resilience-based differentiation; reliability; risk; value-at-risk**

Network resilience is defined as survivability to random failures affecting connections in communications and computer networks. The failures relate to nodes (hardware failures of routers, crossconnects, etc.) or links (fiber cuts or transponder faults). Although not malicious, the failures are still destructive to networks, both from the technical and business viewpoint. To provide resilience, automatic recovery procedures must be designed. These procedures bypass fault-affected elements by redirecting traffic to spare resources. The redirection can be done in various ways, taking into account client needs, regulations, and costs imposed on operators. These aspects are mutually traded-off, and it is necessary to find a balance between them all. On the technological level, this is achieved by using roughly defined service classes, a method known as service differentiation. However, this approach is not always optimal as service provisioning is led by the business rather than technological conditions. The method of designing and managing engineering systems focusing on business aspects of adverse events such as failures is known as risk engineering and management. Here, we show how risk-related aspects can be incorporated in the design and management practice.

The topic is presented with the usage of the most general framework of commonly accepted risk management cycle, as presented in Fig. 1. The keynote presents all the relevant aspects of the cycle, that is:

- risk assessment: identification of types of risks, quantification of their impact, and communication of the assesement results between technical and business staff;
- planning of the risk response: identification of the methods to deal with the recognized risks, and ways to obtain the optimal decision conforming the policies assumed in a selected business;
- response deployment, and risk monitoring.

Along the keynote presentation, we focus first on giving the context and justification for necessity to deal with risk engineering in the contemporary resilient networks. Then, we describe the assessment methods used in the network

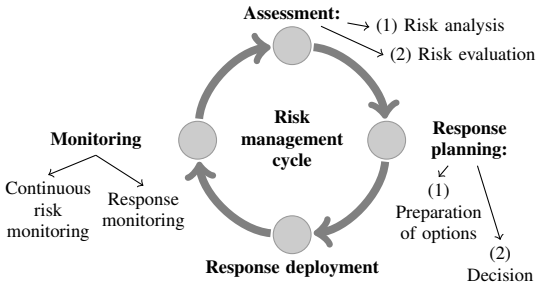

Figure 1. Simplified risk management cycle [1].

design along with the selection of the business-relevant risk metrics (like Value-at-Risk) as well as compensation policies. The latter form a basis for mapping between technical loss and business-relevant measures (e.g., penalties established in Service Level Agreements), where the basic three are as follows: (a) cumulative downtime, (b) total number of outages, (c) mix of the preceding, e.g., number of failures for which downtime exceeds a given threshold. Afterwards, we focus on a spectrum of possible recovery methods along with their performance described from the technical viewpoint. We consider various methods to deal with risk in general, where special emphasis is put on the following risk mitigation strategies like: (a) risk acceptance, (b) risk minimization, (c) profit maximization, and (d) total benefit coverage. Apart from presenting the general trade-offs between risk impact and budget devoted to deacresing this impact, we also relate the risk response planning to the modern portfolio theory.

We end the keynote by discussing challenges that should be faced to establish the full risk management cycle in the resilient networks design adapting contemporary results obtained in the economy and engineering, and propose various research avenues to reach this goal.

ACKNOWLEDGMENT

This scientific work was financed by the Polish Ministry of Science and Higher Education from the research budget for 2013-2015, Project No. IP2012 022972.

REFERENCES

[1] P. Chołda, E. L. Følstad, B. E. Helvik, P. Kuusela, M. Naldi, and I. Norros, "Towards Risk-aware Communications Networking," *Rel. Eng. Sys. Safety*, vol. 109, pp. 160–174, Jan. 2013.