# 4. Analysis

## 4.1 Robustness

The goal of our analysis was to test the robustness of the Swiss Railway network, or in other words, to test the behaviour of the network in case of failures. For this purpose we created a simulation where either nodes or edges were « attacked » and as a consequence were removed from the network. With this model we observed the development of the giant component in the network.

## 4.1 Random vs targeted attacks

## 4.2 Attacks on nodes vs. Edges

## 4.3 Comparison to random networks

References ?

Random graph models are frequently used to predict the behaviour of networks with pretended characteristics. These characteristics are for example the degree distribution or the global clustering in the network. To compare the behaviour of the Swiss Railway network to failures, we used an Erdös-Renyi (ER) random model as well as a Barabási-Albert (BA) random model.

When creating an ER random model a graph with a given number of nodes is generated. Between every pair of node, with probability p, an edge is added to the graph. This random generated model are characterized by a degree distribution, which followas a poisson distribution with <k> = n\*p as well as a clustering coefficient close to the edge creation probability p.

The degree distribution of many networks observed in reality do no not follow a poisson distribution. Therefore the need for random models with different characteristics arises. Often observed networks follow a power-law distribution of node degrees. The power-law distribution is characterized by the existence of a very high number of low-degree nodes and the existence of few nodes with very high degree. Since the Swiss Railway network has a high number of nodes with degree equal to two and only a few nodes that have a degree up to 7, it might be worth to compare the network to a random graph following a power-law distribution. An example of such a random graph is the BA model. This model incorporates the two mechanisms «growth » and «preferential attachment» which are often observed in reality and lead to power-law distributions. The nodes in the BA random graph are created one after another and every new node is connected to a given amount of existing nodes, where nodes with higher degree are preferred.

The theoretical characteristics of the two random graph models suggests that ER graphs are equally vulnerable to random as well as targeted attacks. BA graphs on the other hand are more vulnerable to targeted attacks than to random attacks. That is because when the nodes fail randomly, the probability is high, that a low degree node fails. In contrast targeted attacks might aim at high degree nodes.

# 5. Results