Survivability of Multiple Fiber Duct Failures

D.A. Schupke, A. Autenrieth, T. Fischer
Munich University of Technology
Institute of Communication Networks
80290 Munich, Germany
Tel.: +49 89 289-23500, Fax: +49 89 289-23523
{Schupke,Autenrieth,Fischer}@lkn.ei.tum.de

Abstract

This paper deals with multiple failures of fiber ducts. We study their impact on a network and on several generic resilience schemes and conclude that the impact is significant in particular for large networks. We further recommend where multiple failures can be taken into account in the network design and operation. For this we develop a framework to classify recovery of multiple failures.

1 Introduction

Today's transport networks primarily assure survivability of single failures at a time. As size, integration and complexity of these networks increase, multiple failures become more probable during the operation of the system. Resilience schemes can be unable to survive certain combinations of simultaneous failures in the network. This paper deals with multiple failures of fiber ducts. First, we study their significance in a network in Section 2. Section 3 continues with the impact of multiple failures on several generic resilience schemes. As a result we develop in Section 4 a framework for multiple failure recovery. In Section 5 we draw some conclusions.

2 Significance of Multiple Failures in a Network

In this section we consider the presence of multiple fiber duct failures in different sample networks. We do not take failures of other elements (e.g., nodes, amplifiers) into account. By this we are independent of the technology used and the results we obtain present a lower bound on the probability of multiple failures.

First we consider the Mean Time Between Failures (MTBF) of a fiber duct unit. We assume this basic unit to be one kilometer. Values for MTBF are hard to obtain from literature. The values which can be found may be classified in three different groups: (1) purely hypothetical values, taken as a reference, (2) values taken from real operator measurements over a long period of time or (3) values from standardization which present target values for equipment vendors and network operators. We use in our studies the following values for MTBF:

$\mathbf{MTBF_1}$ A value of 114 failures in 10^9 hours per kilometer cable has been used for the studies in [1], resulting in a MTBF of 1000 years.

$\mathbf{MTBF_2}$ Reference [2] specifies a MTBF of 570 years per optical trunk cable kilometer. This value is an average of statistics provided by European network operators in the RACE project FIRST.

$\mathbf{MTBF_3}$ A cable cut failure rate of 4.39 per year per 1000 sheath miles is provided by [3] based on Bellcore rates. We obtain an approximate MTBF of 367 years per kilometer.

Fiber networks are repairable systems with a Mean Time To Repair (MTTR). The values of the MTTR are depending on a variety of influence factors such as duct type (aerial, underground or submarine cable), failure location (city area or rural/hard-to-reach areas), type of the damage and, of course, reaction and completion times defined in contracts with responsible repair companies. In the following we use MTTR values from a range of 1 hour to 48 hours.

We assume both MTBF and MTTR to be the same throughout the network. Thus a fiber duct unit has the availability

$$a = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}.$$

A complete fiber duct i connecting two nodes in a network is a series connection of l fiber duct units and thus has an availability of $A_i = a^l$.

In our study we consider three sample networks:

nsf-net The NSF network as used in [4] (14 nodes, 21 ducts) spans major US cities.

eur-net A version with 11 nodes and 25 ducts of the pan-European network as used in the COST 239 project [1].

ger-net A national-scale network interconnecting 10 cities in Germany by 13 ducts.

We are interested in the probability P of multiple failures present in the network. We easily obtain this through the complementary probability using the probabilities of no or one failure in the network:

$$P = 1 - \prod_i A_i - \sum_i (1 - A_i) \prod_{j \neq i} A_j$$

Hence, the mean time of multiple failures per year is $T = 365 \times 24 \times P$ hours.

Figures 1 and 2 depict T over a MTTR range of 1 hour to 48 hours for the **nsf-net** and **ger-net** networks. Similarly Figure 4 contains the T-curves for $\mathbf{MTBF_3}$ and $\mathbf{MTBF_2}$. If the MTTR takes values of one or two days, for all networks considerable periods of multiple failures can be determined. In the larger **nsf-net** and **eur-net** networks one has to cope with multiple failure times in the order of hours, even if the repair time is low (~ 5 hours).

Therefore in particular for large networks the network operator has to consider simultaneous failures. One improvement is to reduce the MTTR by making the repair process faster or by contracting several responsible repair companies which can also work on multiple failures in parallel. Another improvement is to take multiple failures into account during the network planning process (see Section 4).

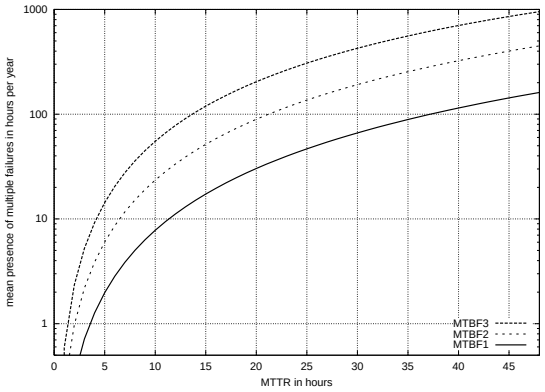


Figure 1: Mean time T of multiple failures per year in the **nsf-net** network over the MTTR of a fiber duct.

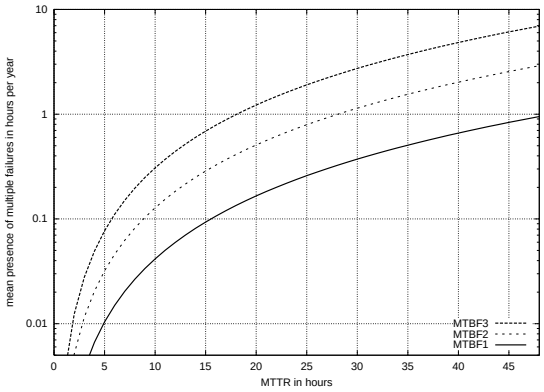


Figure 2: Mean time T of multiple failures per year in the **ger-net** network over the MTTR of a fiber duct.

3 Multiple Failures Survivability of Resilience Schemes

Similar to Section 2 this section deals with the presence of multiple fiber duct failures, however, such that a resilience mechanism cannot survive. Different resilience schemes can be deployed in a network. Table 1 lists when several generic resilience schemes cannot survive multiple failures. For each of these resilience mechanisms we can give an approximation on the probability of not being capable to survive multiple failures.

Table 1: Resilience schemes and their survivability of multiple fiber duct failures.

Scheme [5]	Does not survive multiple fiber duct outages
1+1 and 1:1 connections	at least one failure on primary path and at the same time at least one failure on secondary path
self-healing ring	at least two failures on the ring
rerouting	if not enough spare capacity available
p-cycles [6]	if not enough spare capacity available

1+1 and 1:1 connections

A 1+1 or a 1:1 connection between source node s and target node t is provisioned by two (disjoint) paths in the network. Of course, the most available path between s and t (with availability A_m) represents an upper bound for the availability of any path between between s and t. Thus the upper bound $\hat{A}_p$ of the availability A_p of the pair of the disjoint paths is given by $\hat{A}_p = 1 - (1 - A_m)^2 \geq A_p$.

A shortest-path algorithm can calculate the most available path by setting the metric of a link i to $\log(A_i) = l_i \log(a)$ or directly to the link's length l_i, since the availability a of the fiber duct unit is constant.

Figure 4 contains the lower bound on the unavailable time of a pair of paths (via $365 \times 24 \times (1 - \hat{A})$), i.e. there is at least one failure on primary path and at the same time at least one failure on secondary path. The time bound is an average over all paths between all node pairs. The picture shows this for the **eur-net** network over the MTTR of a fiber duct. For MTTR values ranging from one day to two days, significant outage times of some minutes can be recognized.

Self-healing rings

We deploy the **eur-net** network with six rings from [7] depicted in Figure 3. As an approximation on the probability of not surviving multiple failures we took all possible double failures into account, triple or more failures are neglected. For each of these double failures we looked if there is a ring where both failures are situated. As a ring protects single span failures only, at least one pair of nodes on the ring cannot be connected anymore. From the network point of view the probability for this event gives us a contribution to the probability that there can be user whose connection cannot survive.

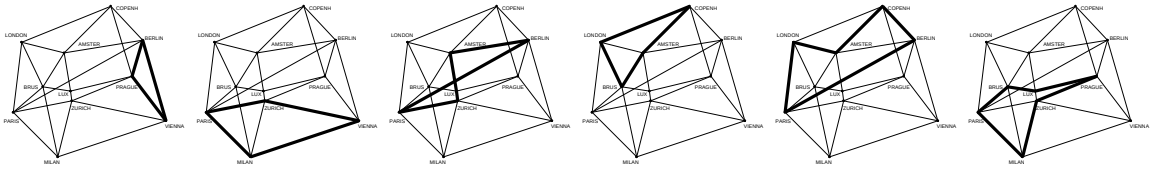
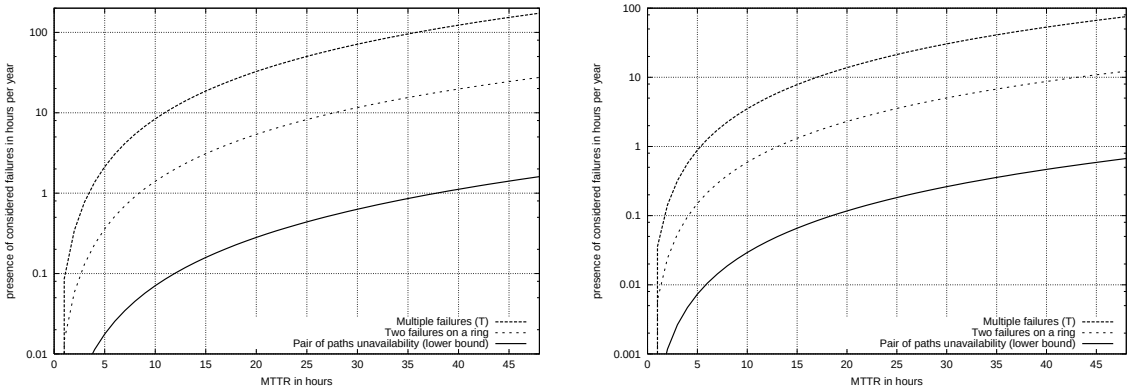


Figure 3: The **eur-net** network with six rings as in [7].

Corresponding to this probability the mean outage time is shown also in Figure 4. It becomes obvious that for MTTR values greater than 15 hours the network operator has to expect periods of double failures affecting a single ring in the order of hours.

Rerouting and p-cycles

From the network point of view, if we take the stringent assumption that the network has enough capacity only for at most one failure, there can be cases where some traffic is lost in presence of multiple failures. Thus the probability of traffic loss corresponds to the probability of multiple failures (Section 2). As many networks are two-connected, it is not possible to protect these networks fully against double or more fiber duct failures.



$\mathbf{MTBF_3}$=367 years $\mathbf{MTBF_2}$=570 years

Figure 4: The mean time T of multiple failures per year, the average time of two failures present on at least one ring, and the lower bound on the time a pair of paths is affected by multiple failures in the **eur-net** network over the MTTR of a fiber duct.

The results indicate that the discussed protection schemes are subject to multiple failures. Therefore from the user's point of view service level agreements (guaranteeing a certain level of availability and repair times) should consider multiple failures. Appropriate extensions agreeing on secondary failure measurements according to Section 4 can be included.

4 A Framework for Multiple Failure Recovery

In the previous sections network-wide significance of multiple failures as well as the vulnerability of different recovery mechanisms in a network was shown. In this section a framework for the recovery of multiple failures is defined.

Recovery mechanisms are commonly classified into protection, distributed restoration and central restoration (e.g., configuration by a central routing system) according to two criteria: the time of the backup route calculation and the type of switching control instance (see Figure 5).

Recovery scheme	Protection	Distributed restoration	Centralized restoration
Backup route setup	preplanned	on-demand	on-demand
Switching control	distributed	distributed	centralized

Additional options:

Recovery scope	local	⟷	global
Resource usage	dedicated	⟷	shared
Resource allocation	prereserved	⟷	on-demand

Figure 5: Classification of recovery mechanisms.

It should be noted that protection schemes are more vulnerable to multiple failures than restoration schemes since they use predefined recovery paths. If the primary failure in a network affects the protection path of a connection, the connection cannot be recovered if affected by a second failure on the working path. Secondly, if the connection was affected by the first failure and was recovered using the protection path, a second failure on the protection path disrupting the connection cannot be recovered.

Restoration schemes on the other hand are inherently more robust against complex multiple failure scenarios. The alternative path is either computed centrally or searched using a distributed flooding mechanism. Therefore, provided that enough spare capacity is available in the network, alternative paths can be found. This should be taken into regard already in the network planning process by including multiple failures into the set of anticipated failure scenarios.

Additional classification can be done depending on the scope of the recovery. In case of a local recovery scope the recovery switching is done in the nodes adjacent to the failure, while in global recovery the switching is done at the connection end-points and partially within the network (e.g., mesh restoration). Examples for local recovery mechanisms in the Optical Transport Network (OTN) are OMS-DP, OMS-SP, OMS-DPRing and OMS-SPRing. Examples for global recovery are OCh-DP, OCh-SP, OCh-DPRing, OCh-SPRing and OSNCP and mesh protection mechanisms.

Finally, the recovery schemes may use dedicated resources, where the backup resources are explicitly reserved for dedicated working connections, whereas with shared recovery the recovery resources can be shared between multiple working connections [5, 8].

The classification of recovery mechanisms takes only the behavior for single failures into consideration. In Figure 6 a framework is defined to classify recovery of multiple failures.

Horizontal approach	Vertical approach
• Network partitioning • Pre-computed recovery (before first failure) • Re-computed recovery (after first failure) • Re-Restoration (After secondary failures)	• Recovery at higher layer (Escalation strategy with hold-off time) • Recovery at lower layer (OMS-Restoration) • Central reconfiguration (by NMS with access to several layers)

Figure 6: Multiple failure recovery framework.

Two approaches are distinguished: a horizontal approach, where the secondary failures are recovered at the same layer (but possibly with another recovery scheme) and a vertical approach, where secondary failures are recovered at another layer.

A second criterion is the point in time when the alternative route for a secondary failure is computed (before primary failure, after primary failure, after secondary failure).

4.1 Horizontal Approach

Network partitioning

A horizontal partitioning of the network in protected domains can be used to minimize the probability of multiple failures. Examples for network partitioning are multiple interconnected rings.

A main consideration to handle multiple failures is the computation of the route to be able to recover from a secondary failure in presence of a primary failure. Three different options can be distinguished:

Pre-computed recovery (before first failure)

In case of pre-computed multiple-failure recovery the alternative paths of secondary failures are calculated already before a primary failure occurs. This option is useful for protection or centralized restoration mechanisms.

Practical approaches for this scenario are protection tables with multiple entries, where a node has to select a protection entry which is still available after a failure. In the planning process the protection routes should be selected to be maximally disjoint, in order to maximize the probability that there is still a protection path available for an arbitrary failure scenario. A second approach could be to compute a second protection table per node for every single link and/or single node failure. In case of a first link or node failure, all nodes load the corresponding secondary protection table.

Re-computed recovery (after first failure)

In this case the secondary alternative paths for working and backup paths affected by a primary failure are calculated after the primary failure.

After the occurrence of a first failure, the network management system or the nodes compute new protection paths for all affected working paths and new alternative paths for all affected protection paths. Figure 7 illustrates this. In the left part of the figure the working path W-1 running over the path G-E-F-D is affected by a failure and switched over to the protection path P-1 running over G-H-I-D. Since this connection is now vulnerable against secondary failures, a backup path P'-1 is recomputed for this connection, running in the example over G-E-B-C-F-D.

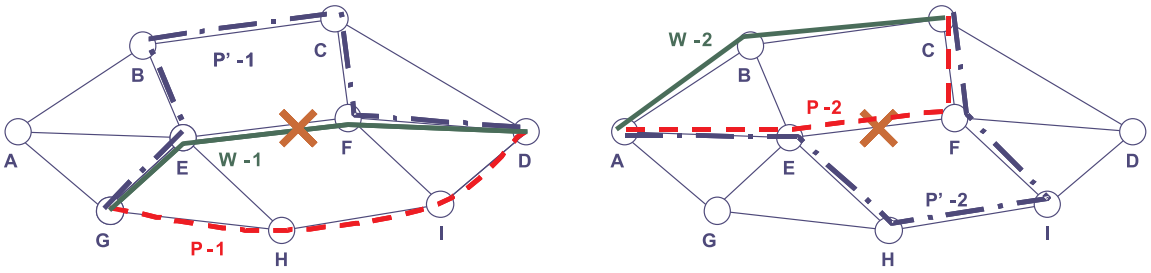


Figure 7: Two possibilities of a protection path recomputation.

In the right part of the figure the situation is shown where the backup path is affected by a failure (P-2). In this case the working path W-2 is also unprotected against secondary failures. Therefore the protection path P'-2 is re-computed.

This multiple failure recovery option corresponds to a protection mechanism in the single failure scenario. The network is protected against multiple failures after a relatively short re-computation phase.

Re-restoration (after secondary failures)

Corresponding to single failure restoration, the alternative route computation for secondary failures could be done on-demand after the occurrence of a secondary failure. Note that in this case the primary recovery mechanism can also be a protection scheme.

4.2 Vertical Approach

Different transport technologies can participate in the recovery of a failure. However, the logical layers (e.g., OTN and SDH) would by default not coordinate themselves when attempting recovery from outages. On the one hand, server layer(s) are left unaffected by client layer failures for the most part. On the other hand,

due to dependency on lower-layer services, client layers are in most cases affected by failures on the layer(s) below, which can inherently cause multiple simultaneous failures.

Recovery at higher layer (escalation strategy with hold-off time)
Recovery in such systems with vertical separation may converge to a steady state relatively slow or not at all. A simple, but certainly sub-optimal solution is to introduce escalation tactics [5]. A server layer is given the opportunity to solve the problem during a certain period of time. When the hold-off timer expires, a client layer recovery is performed if the measures had no effect so far. Further escalation or interworking strategies are described and compared in [8].

As an alternative, explicit failure messaging across layers can be introduced. Besides standardized failure types/messages, this would also include failure localization procedures. Based on knowledge about the capabilities of the given layers, recovery can be explicitly delegated or executed, respectively, by a generalized control plane. This is currently pursued by the GMPLS standardization effort, albeit the various transport technologies are logically merged to a uniform infrastructure layer [9] rather than attempting vertical messaging across layers. ANSI and OIF also work on layer coordination [5].

Recovery at lower layer (OMS-restoration)
A second option for a vertical multiple failure recovery approach works on two granularities, namely on path (e.g., a protected OCh or an unprotected OCh carrying a protected SDH/SONET signal) and line (e.g., OMS) layers, respectively [5]. The first occurring failure is quickly overcome on the fine-granular (higher) level. Shortly afterwards the failure is repaired with a slower restoration mechanism on the level below using optical crossconnects (OXCs). The higher layer can now perform a protection reversion. That way the network is protected against a secondary failure.

A drawback is, that with the mechanism described in [5] the revertive switching of the higher layer recovery mechanism causes an additional short-term disruption of the already recovered connections.

Central reconfiguration (by network management system)
With a network management system (NMS) resource optimization is performed on the network, trying to accommodate all demands with the current topological restrictions in mind. Therefore, a centralized entity recomputes and updates routing in the network. The network management system has the advantage to access several layers for service restoration.

5 Conclusions

We discussed the significance of multiple failures for a network and for several generic resilience schemes by looking at the mean time of multiple failures per year. Their impact is significant in particular for large networks.

Therefore network operators should consider simultaneous failures in the formation of the repair procedures and/or during the network planning process. Also service level agreements should include a consideration of multiple failures.

We further developed a framework to classify recovery of multiple failures. We distinguish between a horizontal approach and a vertical approach according to the recovery scope of a single layer or of multiple layers, respectively. The horizontal approach includes network partitioning, pre-computed recovery (before first failure), re-computed recovery (after first failure) and re-restoration (after secondary failures). The vertical approach comprises recovery at higher layer (escalation strategy with hold-off time), recovery at lower layer (OMS-restoration) and central reconfiguration (by network management system).

In further work it becomes interesting to consider the time between the occurrence of a single failure in the network and a subsequent one. This provides a requirement for the time the second line of defense has to be active.

Acknowledgments

The authors would like to thank R. Prinz for some of the implementations. This work was supported by the German Federal Ministry of Education and Research (BMBF) in the project TransiNet (`http://www.transinet.de/`).

References

[1] P. Batchelor et al. Ultra high capacity optical transmission networks: Final report of action COST 239. `http://web.cnlab.ch/cost239/`, 1999.

[2] D. Gardan et al. Availability analysis of the optic local loop. In *EFOC & N*, 1994.

[3] M. To and P. Neusy. Unavailability analysis of long-haul networks. *IEEE JSAC*, 12(1), January 1994.

[4] R. Ramaswami and K. N. Sivarajan. Design of logical topologies for wavelength routed optical networks. *IEEE JSAC*, 14(5), June 1996.

[5] O. Gerstel and R. Ramaswami. Optical Layer Survivability—An Implementation Perspective. *IEEE JSAC*, 18(10), October 2000.

[6] W.D. Grover and D. Stamatelakis. Bridging the ring-mesh dichotomy with p-cycles. In *Second International Workshop on the Design of Reliable Communication Networks (DRCN 2000)*, 2000.

[7] P. Arijs, M. Claeys, and P. Demeester. The design of SDH ring networks using Tabu Search and Simulated Annealing. In *5th International Conference on Telecommunication Systems*, 1997.

[8] P. Deemester et al. Resilience in Multilayer Networks. *IEEE Com. Mag.*, page Aug, 1999.

[9] J.P. Lang et al. Link Management Protocol (LMP). Internet Draft `draft-ietf-mpls-lmp-02`, Mar 2001. Work in progress.