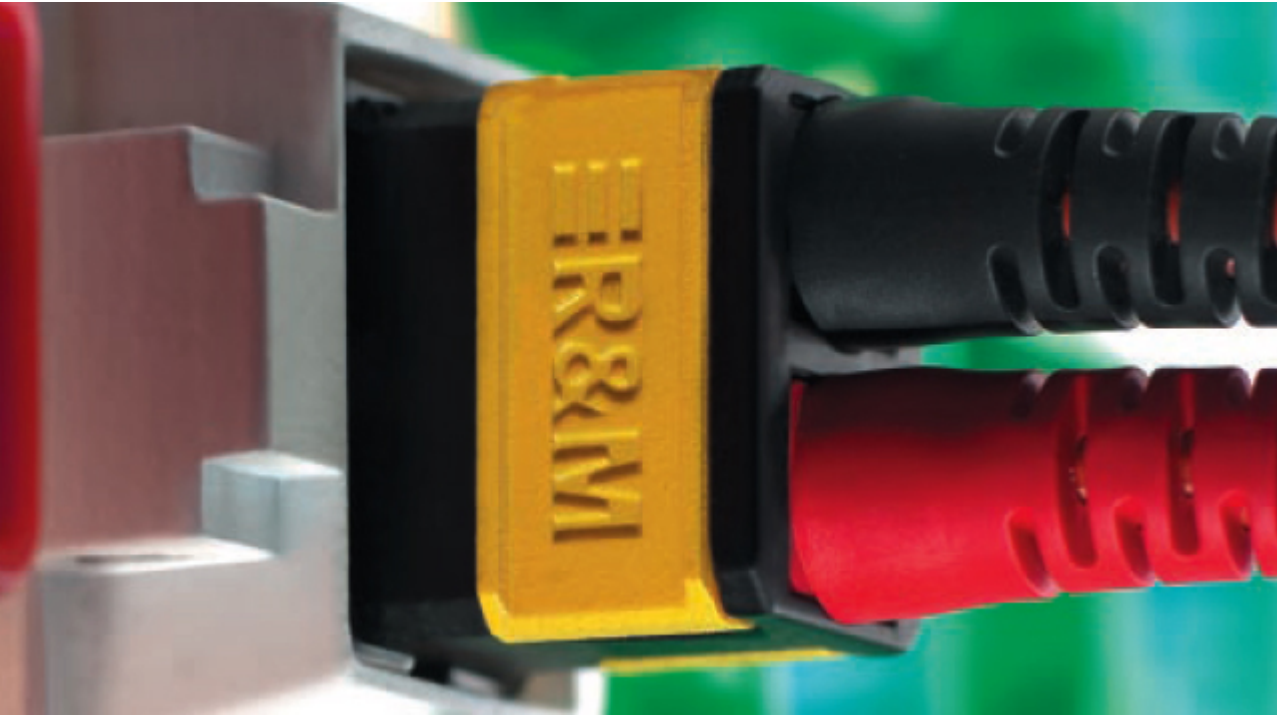


White Paper



Safety gaps in the LAN?

A fear of the big blackout clouds the view
to the many small risks



Convincing cabling solutions

Contents

Security gaps in the LAN?

A fear of the big blackout clouds the view
to the many small risks

1. A LARGE BLACKOUT OR MANY SMALL LOSES?	3
2. HOW LONG CAN YOUR ENTERPRISE SURVIVE A NETWORK BREAKDOWN?	4
3. NETWORK SAFETY - A QUESTION OF PRIORITISING?	4
4. ELIMINATING PRINCIPLE SOURCES OF ERRORS.....	5
5. FLEXIBILITY AND SAFETY - CONTRADICTIONARY DEMANDS	7
6. SETTING THE COURSE ALREADY AT THE PLANNING STAGE	7

© Copyright 2004 Reichle & De-Massari AG (R&M). All rights reserved.

The transmission or copying of this publication or extracts thereof, for whatever purpose and in whatever form, is prohibited without the prior written permission of Reichle & De-Massari AG. Information contained in this publication is subject to change without notice. Great care has been taken in the preparation of this document which reflects the technical status current at the time of preparation. Subject to technical changes.

Safety gaps in the LAN?

Viruses, worms and Trojan horses frequently make headlines, with damage to large enterprises often reported to be in the hundreds of millions of dollars. However, not all those responsible for IT matters are aware of the fact that most of the network incidents are caused by unspectacular connection errors. This represents money that does not disappear in a sudden opening of the floodgates, but that seeps away gradually.

Connection errors result from technical deficiencies, human error or wilful interference. Effective protection against all three causes is available – with the right technology.

Business segment:	Enterprise Cabling
Application:	Local Area Networks (LANs), connection technology
Format:	White Paper
Topic:	Security in local networks through measures to prevent unintended or unauthorised interference with the connections
Objective:	Provide information on the principal causes of network incidents, their effects and prevention
Audience:	IT managers, planners and installers; IT consultants
Author(s):	Thomas Bürgler
Published:	July 2004

1. A large blackout or many small losses?

After September 11, 2001, disaster recovery planning became the buzz-word among IT managers, predominantly in the US, who checked their networks for security so as to ensure business continuity should the worst come to the worst. However, the electricity blackouts of 14 August 2003 in the north of the US and at the end of September 2003 in Italy had far more severe consequences for enterprise networks, but there was no comparable flurry of activity – perhaps because these events were not associated with terrorism.

In Europe, September 11 did not trigger a comprehensive increase in security efforts. According to a survey published in the weekly computer magazine «Computerwoche» of 20 November 2001, only 9 % of enterprises reacted strongly to these events, while 66 % did not react at all with additional safety measures. In the meantime, security savings are commonplace again worldwide. This trend is confirmed by the results of a survey, of August 2003 by Ernst & Young, on the topic of IT security in enterprises.

At the same time, the number of security infringements is clearly on the increase – a fact which according to the current study «IT Security 2004» carried out by Information Week has only caused about one in three enterprises to increase their safety measures.

It is useful to differentiate between a catastrophic event and many lesser failures and malfunctions in everyday operations. Viruses, worms and Trojan horses frequently make headlines. However, targeted attacks from the outside are usually isolated incidents; they only become newsworthy if they cause a certain amount of damage. In contrast to this, the fact that most network failures are caused by hardware faults, including cabling faults, remains largely unnoticed because it is less spectacular. Nevertheless, well-known studies have been emphasising this very problem.

2. How long can your enterprise survive a network failure?

For 46 % of enterprises a network failure of one hour's duration equates to an economic loss of up to 50,000 US dollars; for 8 % of enterprises the loss exceeds the million USD mark. 4 % of enterprises fear for their existence when the network is down for one hour; after 72 hours, the last 40 % of enterprises are also endangered. These figures were obtained in spring 2001 by Contingency Planning Research in a survey to which 163 enterprises responded.

Further statistics show that stock market transactions and payment transactions with credit cards react most sensitively to network failures and data loss – followed by energy supply, telecommunications, transport and traffic, as well as large production facilities.

A conclusive IT security concept is thus based on a thorough risk analysis. Parameters such as the likely extent of damage, frequency of occurrence and the value of endangered assets all play a part, as does the nature of attacks or malfunctions, for example viruses, unauthorised access, denial-of-service attacks, and manipulation. Further parameters include the possible attackers themselves, be they computer hackers, terrorists, authorised or unauthorised employees, former employees, competitors etc. Such a risk analysis gives those responsible for IT a clear idea of the crucial parts of an enterprise and their potential exposure to danger, and provides the starting point for effective protection.

Model calculation

Economic loss caused by faults in lines and connections

On average, 1 hour of network failure in sensitive areas of enterprises causes an economic loss of 90,000 USD (Contingency Planning Research).

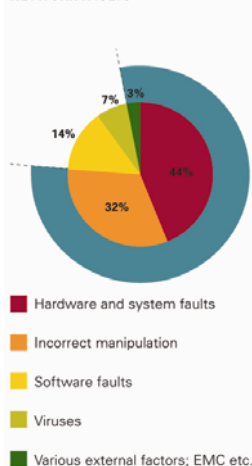
72 % of all systems in sensitive areas have failure downtimes totalling 9 hours per annum (The Standish Group).

59 % of network problems can be directly attributed to the physical infrastructure and connections (The Gartner Group).

Thus the economic loss caused by faults in lines and connections is $0.72 \times 90,000 \text{ USD per hour} \times 9 \text{ hours per annum} \times 59 \% = \mathbf{344.088 \text{ USD per annum}}$.

3. Network safety – a question of prioritising?

CAUSES OF DATA LOSS AND NETWORK FAULTS¹⁾



The study from Contingency Planning Research shows that only 7 % of data loss is caused by viruses, while 44 % is caused by hardware faults and 32 % by human error. The latter two segments can more or less be attributed to layer 1 (the teal-coloured area in the illustration on the left).

The majority of incidents involving everyday network incidents and data loss are thus caused by minor faults in operation and by human shortcomings. These incidents do not threaten an enterprise's existence, but they can still have serious consequences, for example temporary standstill of parts of the production because a new PC terminal has been incorrectly connected and paralyzes the network; or the order processing department cannot take any orders because the server is being irritated by an incorrectly connected terminal. Even if it is "only" the LAN connector which was mistakenly pushed away by a broom during cleaning and was subsequently plugged in incorrectly, valuable work time is lost until the fault is detected and remedied.

Periods of time lost because the network happens to be slow again are not counted. Poor-quality cables, bad contacts and mismatches often lead to repeat transmissions, thus considerably slowing data rates. Not only do they cause standstills but they lead to inefficiency. Technical problems assume economic dimensions.

Clearly, it is rather unlikely that a super MCA will all of a sudden shut down an enterprise. Most enterprises are plagued by many small security leaks – and these are to be found in the physical network.

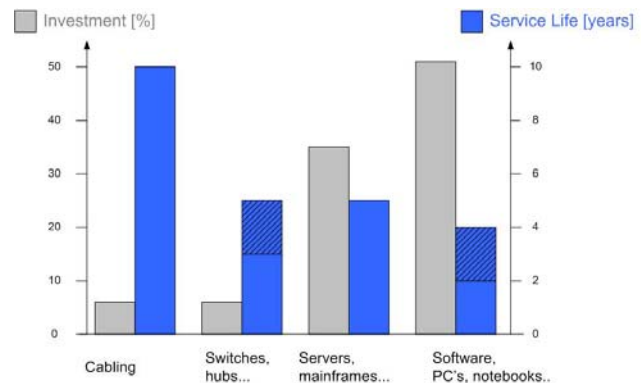
It is therefore difficult to understand that the network should be the very area where cost savings are made. For, according to the IT analyst Datapro, cabling only accounts for approximately 5 % of IT expenditure. Software and hardware account for somewhat over 50 % of the investment; servers and large computers for 35 %; and active devices such as switches and hubs 7 %. A look at the service life of the individual IT segments clearly shows that much more attention should be paid to cabling, which has an expected service life of approximately 10 years. Cabling provides the foundation of every IT infrastructure, with the entire IT network then being built on it. This solid foundation is no different in principle than the equally solid masonry foundation put in place in the construction of a house.

4. Eliminating principle sources of errors

Poor or incorrect connections can often be traced back to three factors: technical deficiencies, human error, or wilful interference.

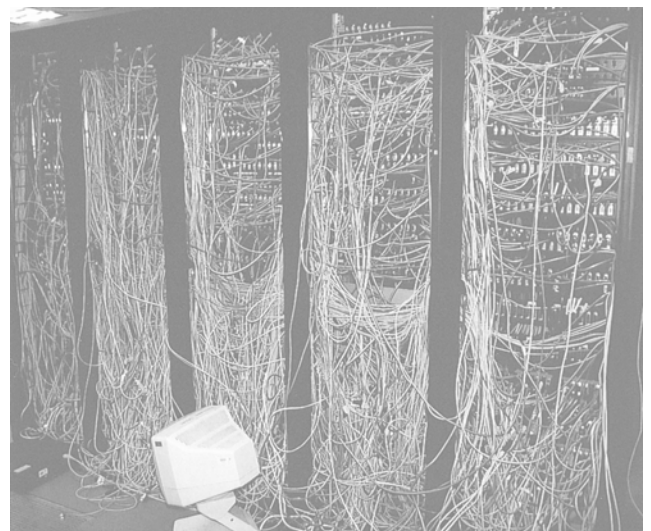
Improved technology helps to prevent technical failures, but this issue also has a human component: the quality awareness of every employee at whatever level.

Conversely, human error can be countered with proper procedures in handling technology: with clear and well-arranged installation and neat documentation. A first step towards this includes unambiguous marking of all network components, connection cables and connectors, for example using a system of colour coding.

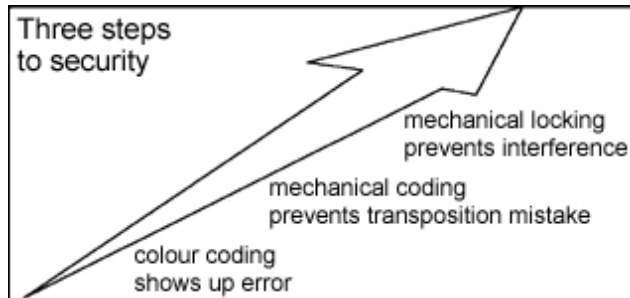


Ratio of investment expenditure to service life in various IT segments. The central importance of cabling is often underestimated.

Source: Datapro / illustration: R&M



With such a “cable mess”, incorrect connections in the local data network are practically pre-programmed. Troubleshooting is almost impossible.



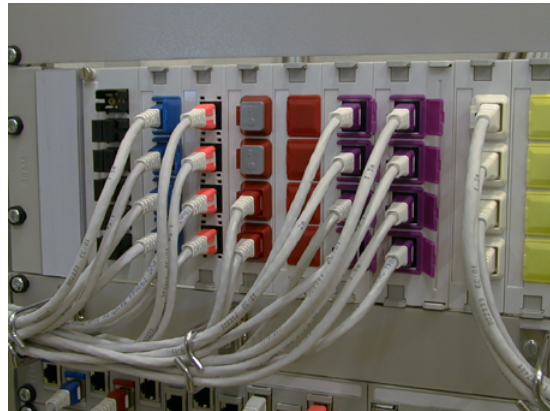
The way to improved security in networks starts with simple protective measures in the areas of cables and connectors. In this way, numerous expensive mishaps and breakdowns can be prevented.

Another step consists of mechanically preventing incorrect connections. This is all the more important since the RJ45 connector is so ubiquitous. Everything seems to fit everywhere: the telephone connection, the Token-Ring workstation, the Ethernet-PC LAN – they all use RJ45 connectors. It may happen that incorrect connections not only interfere with the proper function of networks, but, for example, that the direct current of the telephone network results in sensitive data ports being “fried”.

This is where mechanical plug-in protection with visual coding comes into its own. It makes incorrect connections a thing of the past and prevents undefined states in the network.

The best protection against human error and interference is provided by a system which prevents unintended or intended tampering with network connections and unauthorised access alike. Intrusion detection should not be limited to software which is designed to stop professional intruders and ambitious hobby hackers in their tracks. Many an unauthorised intervention can simply be prevented mechanically.

Such security is essential in emergency services or hospitals where human life is at stake, or in banks, stock exchanges and any enterprises which depend on their networks for business. The best possible security is also highly recommendable in situations where misuse or simply the temptation to play would otherwise keep network administrators busy, for example in schools, libraries and public areas. The same applies to conference rooms, individual workplaces where staff frequently come and go, hotel lobbies or department stores with data connections in outlying areas where cash registers are connected and where people must be prevented from surfing the internet at night at the expense of the enterprise. Such protection is also valuable at home where children play with cables.



Neat cable management. The ports are colour coded, mechanically coded to prevent incorrect plugging, and can be equipped with a protective device which only allows authorised persons to plug or unplug connections.



Mechanically secured outlet at the workplace. No more incorrect connections mean no chance of destroying network cards in PCs.

5. Flexibility and safety – contradictory demands

Once a local network has been installed and readied, it is largely secure in operation. However, a local network is dynamic: terminals are modernised, the topology is expanded, individual workplaces are moved or entire sections are relocated. Experience has shown that each year about 40 % of all employees are involved in some move or other.

Such changes can only be implemented smoothly if the network status is unambiguous at all times. This in turn requires impeccable port management. Authorised staff must be able to install, change or retrofit security components quickly – without the need for major de-installation work.

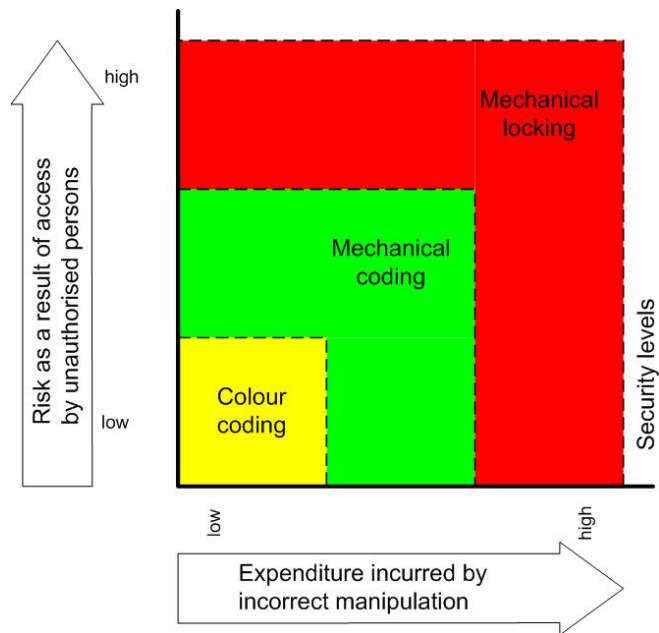
6. Setting the course already at the planning stage

The points discussed above should be taken into account in the early stages of selecting a cabling system for a local data network. Even if no mechanical security products are to be used in the first stage of installation, the option of doing so in the future should be kept open.

The diagram on the right serves as a guide for planning the security of the LAN. Two aspects are of prime importance in the selection of security products: the potential expenditure arising in the case of network failure on the one hand, and the possibility of interference by unauthorised persons on the other hand. Depending on the weighting of these factors, the security levels and thus corresponding products can be determined.

R&M has investigated the topic of security gaps in the LAN in great depth. This has led to the development of a modular system which largely closes potential gaps in a local data network.

For more information, visit us at www.rdm.com



Guide for planning the security of the LAN. The easier it is for unauthorised persons to gain access to network connections, and the riskier network failures are to the enterprise, the higher the security level that should be selected. Diagram: R&M