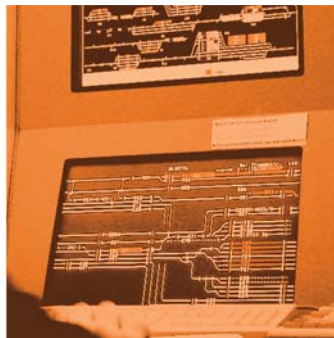


## White Paper



## Bahn-Datennetze – Anforderungen an höchstverfügbare Datennetze der Leit- und Sicherungstechnik bei Bahnen

---

## Inhalt

<b>1. Grundlagen</b>	<b>3</b>
<b>2. Anforderungen an die Leit- und Sicherungstechnik</b>	<b>4</b>
2.1. Erläuterung der CENELEC EN-50126	5
2.2. Erläuterung der CENELEC EN 50159	5
2.3. Die Betriebszulassung	6
<b>3. Sicherheit und Verfügbarkeit der Leit- und Sicherungstechnik</b>	<b>6</b>
3.1. Die Sicherheit	6
3.2. Die Verfügbarkeit	7
3.3. Die Grenzen der Redundanz	8
<b>4. Trends im Bahnen-Sektor</b>	<b>9</b>
4.1. Steigender Bandbreitenbedarf	9
4.2. Leistungsfähige Netzinfrastruktur	10
<b>5. Schlussfolgerung</b>	<b>12</b>

## Bahn-Datennetze

Die technische und wirtschaftliche Optimierung des Netzbetriebs ist eine ständige Aufgabenstellung der Bahnnetzbetreiber. Auf dem Gebiet der Datennetze wurden durch die Standardisierung der Übertragungsverfahren die Voraussetzungen für Optimierungsmaßnahmen geschaffen. So bedienen sich die Systeme der Leit- und Sicherungstechnik für den Bahnbetrieb immer häufiger der bereits vorhandenen Datenkommunikationstechnik, anstatt proprietärer Technik.

Der hohe Automatisierungsgrad heutiger und insbesondere zukünftiger Bahntechnik ist nur unter dem Einsatz von höchst zuverlässigen Systemen zur Informationsübermittlung möglich. Darüber hinaus müssen die Netztopologien die Verfügbarkeitsanforderungen umfassend erfüllen.

Die CENELEC Norm EN 50126 und insbesondere die daraus abgeleitete Norm EN 50159-1:2001 für geschlossene Übertragungsnetze bilden dabei die Basis für die sicherheitsrele-

vante Kommunikation der Sicherungsanlagen der Leit- und Sicherungstechnik von heute.

Die Anwendung neuer Technologien für die wirtschaftliche Betriebsführung steht aber noch am Anfang. Die bisherigen Bemühungen zur Einführung innovativer Technologien wie Local Area Networks (LAN), Wide Area Networks (WAN), IP-Technologie und GSM-R sind ein Beginn, haben aber noch keine wirksamen Ergebnisse gezeigt.

Bis heute werden in der Leit- und Sicherungstechnik nur physikalisch separate Netze oder SDH-Pfade akzeptiert. Andere Mechanismen zur Netztrennung nach EN 50159-1 wie VLAN-Tags oder MPLS-Label werden heute noch nicht für die Zulassung eines Gesamtsystems anerkannt. Um moderne Datenübertragungstechnologien in der Zukunft nutzen zu können, sind in der Norm EN 50159-2 die Grundlagen für die Übertragung über offene Netzstrukturen festgelegt.

### 1. Grundlagen

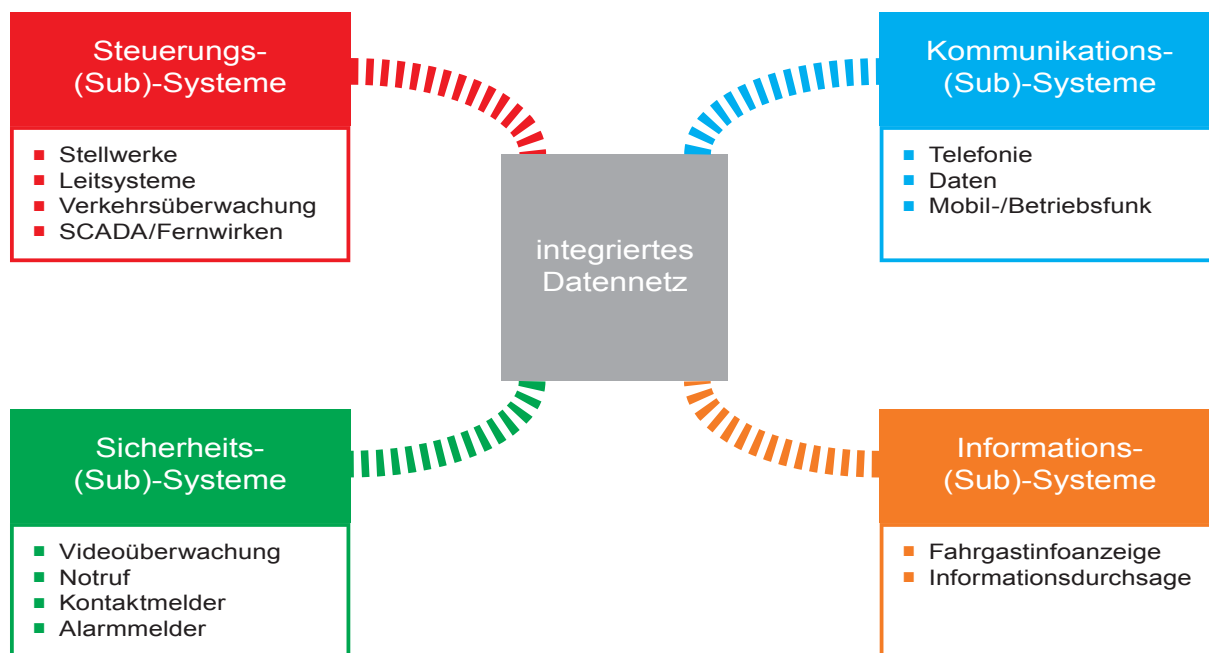
Die Bahngesellschaften in Europa stehen unter dem Druck ihre Unternehmen betriebswirtschaftlich zu optimieren. Dies gilt insbesondere für die Regionalbahnen, die recht häufig durch hohe Betriebskosten einerseits und durch eine geringe Verfügbarkeit an Investitionsmitteln andererseits bedroht scheinen.

Zentrale Bedeutung kommt dabei einem integrierten Konzept zur effektiven und wirtschaftlichen Datenkommunikation der verschiedenen Bahndienste zu.

Der heutige Stand der Datenkommunikation in der Leit- und Sicherungstechnik stellt jedoch zum Teil unterschiedliche Anforderungen an die jeweiligen Anwendungen, mit teilweise verschiedenen Sicherheitsgraden und physikalisch unterschiedlichen Übertragungstechniken. Dies führte bislang dazu, dass in der Regel für einzelne Anwendungsgruppen jeweils separate Netze aufgebaut wurden. Zur Leit- und Sicherungstechnik zählen bspw. Heißläuferortungsanlagen, Achsenzähler, Gleisfreimeldeanlagen und Zungenprüfkontakte.

Auf Grund der unterschiedlichen Randbedingungen und der entwicklungsgeschichtlichen Hintergründe der Leit- und Sicherungstechnik können heute also gleichzeitig noch separate Kabel für die klassische Modemtechnik und leitungsgebundene festgeschaltete synchrone Multiplexsysteme nebeneinander existieren. Netzkonzepte also, welche sich zwar als hoch zuverlässig bewährt haben, aber heute unter Wirtschaftlichkeitsaspekten kritisch zu bewerten sind.

Abhilfe würde schaffen, für die gesamte Datenkommunikation ein einheitliches, integriertes Datennetz zu verwenden und so den Betrieb von parallelen Netzen und Insellösungen zu vermeiden.



Grafik 1: Alle Dienstanwendungen über ein Datennetz

Das integrierte Datennetz bildet das Rückgrat einer effizienten und störungsfreien Mobilität für Passagiere und Güter.

Dabei haben die bisherigen Bemühungen zur Entwicklung und Einführung innovativer Technologien aus dem Bereich IP für solche

integrierte Datennetze in der Leit- und Sicherungstechnik noch keine wirksamen Ergebnisse gezeigt. Das Risiko bei der Einführung und Nutzung solcher Technologien ist aus Sicht der Bahnen heute noch zu hoch.

## 2. Anforderungen an die Leit- und Sicherungstechnik

Die bei den Eisenbahnbetrieben eingeführten technischen End-Systeme, gerade für die Leit- und Sicherungstechnik, haben im Vergleich zu Lösungen beispielsweise in der industriellen Automatisierungstechnik, sehr lange Produktlebenszyklen.

Werden zur Realisierung von Systemen für den Eisenbahnbetrieb Komponenten aus dem „normalen“ Markt verwendet, so kommt es zu einer Diskrepanz zwischen den Produktlebenszyklen der zugekauften Komponenten und den erwarteten Produktlebenszyklen der eisenbahntechnischen Systeme.

Bei der Einführung neuer Technologien und Verfahren für die Betriebsführung von spurgebundenem Verkehr müssen die genauen Verhältnisse und das Umfeld des jeweiligen Anwendungsfalles in Betracht gezogen werden, um einen sicheren und zugleich wirtschaftlichen Betrieb zu ermöglichen.

Systeme der Leit- und Sicherungstechnik für den Bahnbetrieb bedienen sich in großem Umfang der Datenkommunikationstechnik. Eine zentrale Rolle bekommt dabei die Darlegung von Übertragungssicherheit und Dienstqualität.

Das Europäische Komitee für elektrotechnische Normung (CENELEC) hat die Norm EN-50126 und insbesondere die daraus abgeleitete Norm EN 50159-1:2001 für geschlossene und akzeptierte Übertragungsnetze definiert. Diese Normen bilden die Basis für die sicherheitsrelevante Kommunikation der Sicherungsanlagen der Leit- und Sicherungstechnik.

Die Systeme der Sicherungsanlagen benötigen eine Betriebszulassung, um im Bahnbetrieb eingesetzt werden zu können. Diese Betriebszulassung steht dabei immer am Schluss eines umfangreichen Zulassungsverfahrens. Die Betriebszulassung erfolgt länderspezifisch gemäß der CENELEC EN-50126.

## 2.1. Erläuterung der CENELEC EN-50126

CENELEC steht für „Comité Européen de Normalisation Electrotechnique“ (frz.), d.h. Europäisches Komitee für elektrotechnische Normung (engl. „European Committee for Electrotechnical Standardization“).

Die CENELEC Norm EN-50126 ist die zentrale Norm für die hier besprochene sicherheitsrelevante Kommunikation. Sie gibt Hinweise für die Spezifikation und den Nachweis von „RAMS“:

- Reliability (Zuverlässigkeit)
- Availability (Verfügbarkeit)
- Maintainability (Instandhaltbarkeit)
- Safety (Sicherheit)

für alle Phasen des Produktlebenszyklus.

Die für die Leit- und Sicherungstechnik eingesetzten technischen Ausrüstungen sollen dafür sorgen, dass bei einem Fehlverhalten des

Menschen das Risiko einer Gefährdung hinreichend klein gehalten wird. Voraussetzung hierfür ist, dass die Technik zum Zeitpunkt des Fehlverhaltens funktionsfähig ist. Die sich hieraus ergebenden Anforderungen (z. B. Fehleroffenbarung und Verhinderung von Fahrtfreigaben bei nicht gegebener Funktionsfähigkeit der Technik) müssen bei der Systementwicklung berücksichtigt werden. Begriffe wie Sicherheit und Verfügbarkeit von Übertragungsnetzen kommen dabei zum Tragen (siehe auch Kapitel „Verfügbarkeit und Sicherheit der Leit- und Sicherungstechnik“).

Die aus der CENELEC EN-50126 abgeleitete Norm EN 50159-1:2001 für geschlossene Übertragungsnetze bildet die Basis für die sicherheitsrelevante Kommunikation der Sicherungsanlagen der Leit- und Sicherungstechnik.

## 2.2. Erläuterung der CENELEC EN 50159

### EN 50159-1 (Teil 1)

Ein erstes Ziel der Norm ist die sichere Kommunikation in geschlossenen Netzen. Für diese müssen folgende Voraussetzungen gegeben sein:

- Es ist nur autorisierter Zugriff möglich,
- die maximale Anzahl der anschließbaren Teilnehmer ist bekannt und
- das Übertragungsmedium ist bekannt und unveränderlich.

### EN 50159-2 (Teil 2)

In einem zweiten Schritt wurden die Voraussetzungen der geschlossenen Netze für die Definition einer sicheren Kommunikation in offenen Netzen aufgehoben. Das heißt, es wurden folgende Voraussetzungen für ein offenes Netz angenommen:

- Unterschiedliche Übertragungswege und -technologien,
- beliebige Speicherung der Nachrichten und
- möglicher unautorisierter Zutritt zum Kommunikationsnetz.

Diese erweiterten Anforderungen erfordern einen Angriffsschutz und damit zusätzliche Aufwendungen, wie Verschlüsselungsverfahren und Verwaltung der Kryptoschlüssel.

Hierbei geht es weniger um die denkbaren direkten Angriffe auf physische Teile des Systems, wie etwa direktes Anzapfen von datenführenden Leitungen vor Ort. Vielmehr geht es um die Verhinderung der unbefugten anonymen Verbindungsaufnahme von leistungsfähigen Rechnern mit destruktiven Absichten, wie das in einem offenen Datennetz mit einer nicht kontrollierbaren großen Menge von Teilnehmern leicht möglich ist.

Wie Hacker-Angriffe im Internet auf unzureichend geschützte Computersysteme von Banken, Militär usw. zeigen, handelt es sich dabei um ein ernstzunehmendes gesellschaftliches Phänomen mit beträchtlichem Bedrohungspotenzial.

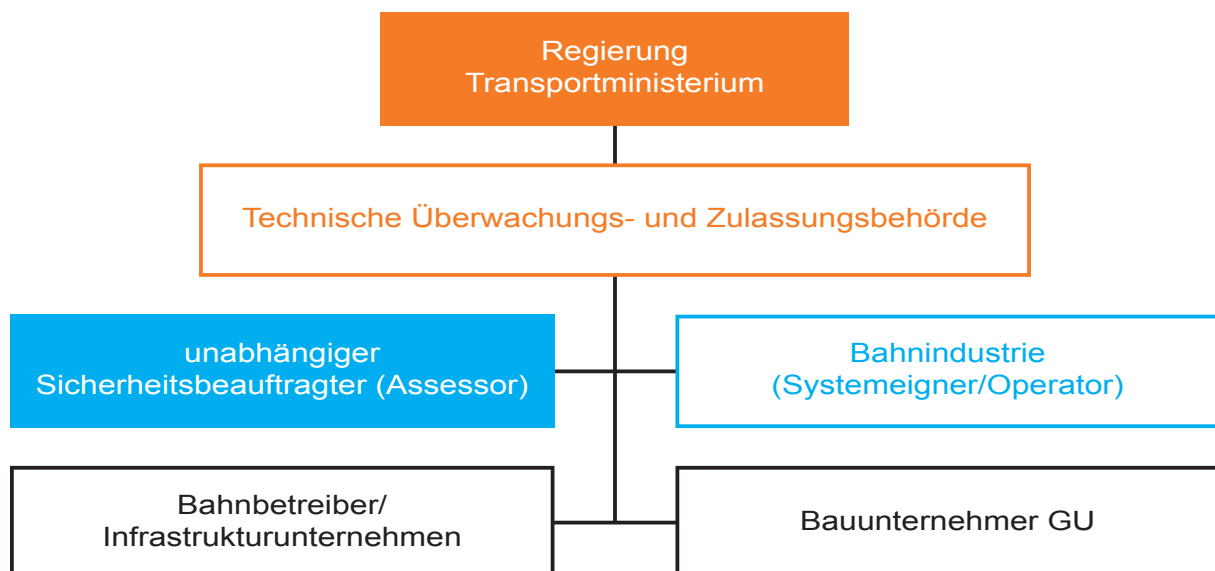
## 2.3. Die Betriebszulassung

Um eine technische Komponente der Telekommunikation im Bereich sicherheitsrelevanter Bahnanwendungen betreiben zu können, muss diese von Amtswegen eine Zulassung erfahren.

Diese sogenannte Betriebszulassung fordert der Bahnnetzbetreiber ein. Die Betriebszulassung ist verbunden mit dem Nachweis der zufriedenstellenden Funktion und anderer Eigenschaften wie z. B. Verfügbarkeit, Umwelteigenschaften und Wartbarkeit der Komponenten unter definierten äußeren Randbedingungen. Dabei spielt die Rückwirkungsfreiheit der Applikations-Software von signaltechnischen,

nicht sicheren Komponenten auf Komponenten mit Sicherheitsverantwortung eine wichtige Rolle. Sie muss von den Komponenten mit Sicherheitsverantwortung gewährleistet bzw. nachgewiesen werden. Dadurch wird verhindert, dass sich Fehler in den signaltechnisch sicheren Komponenten ausbreiten.

Betriebszulassung bzw. Typenprüfung erfolgen länderspezifisch. Im Rahmen der europäischen Standardisierung wird angestrebt, eine gegenseitige Anerkennung der Betriebszulassung der verschiedenen Bahngesellschaften zu ermöglichen.



Grafik 2: Übersicht der beteiligten Parteien im Betriebszulassungsprozess

## 3. Sicherheit und Verfügbarkeit der Leit- und Sicherungstechnik

### 3.1. Die Sicherheit

Die Sicherheit ist eine gesetzlich zu erfüllende Zielsetzung. Eine höhere Sicherheit reduziert das Risiko von Schaden für Mensch, Anlage und Umwelt (z. B. alle Flugzeuge bleiben am Boden). Ein finanzieller Gewinn lässt sich z. B. durch niedrigere Versicherungsprämien erzielen. Sicherheit wird erzielt durch

- Prüfredundanz (integre Systeme),
- Wirkredundanz (persistente Systeme),
- oder Schutzredundanz.

Dabei können die hohen Zuverlässigkeits- und Verfügbarkeitserwartungen an die komplexen Systeme der Nachrichtentechnik nur erfüllt werden, wenn während der Definitions-, Entwicklungs-, Fertigungs- und Nutzungsphase bestimmte Aktivitäten zur Sicherstellung der Qualität und Zuverlässigkeit durchgeführt werden.

Ein Maß für die Zuverlässigkeit wird mit dem MTTF: Mean Time To Fail (mittlere Lebensdauer), z. B. 100 Jahre angegeben.

Dieses Maß bewertet die Wahrscheinlichkeit eines Systems, während einer gegebenen Zeitspanne funktionstüchtig zu bleiben.

### 3.2. Die Verfügbarkeit

Die Verfügbarkeit ist eine ökonomische Zielsetzung. Eine höhere Verfügbarkeit erhöht die produktive Zeit und den Durchsatz (z. B. alle Züge verkehren fahrplanmäßig.)

Der Gewinn kann durch erhöhte Produktivität ausgewiesen werden. Verfügbarkeit wird erzielt durch funktionale Redundanz, welche die Funktion ausüben kann und durch bessere Wartung.

Zur Steigerung der Verfügbarkeit werden bei den in der Leit- und Sicherungstechnik zum Einsatz kommenden Übertragungsnetze und deren Systeme Redundanzen geführt. Die Verfügbarkeit kann auch durch andere Maßnahmen, wie z. B. Wartung gesteigert werden.

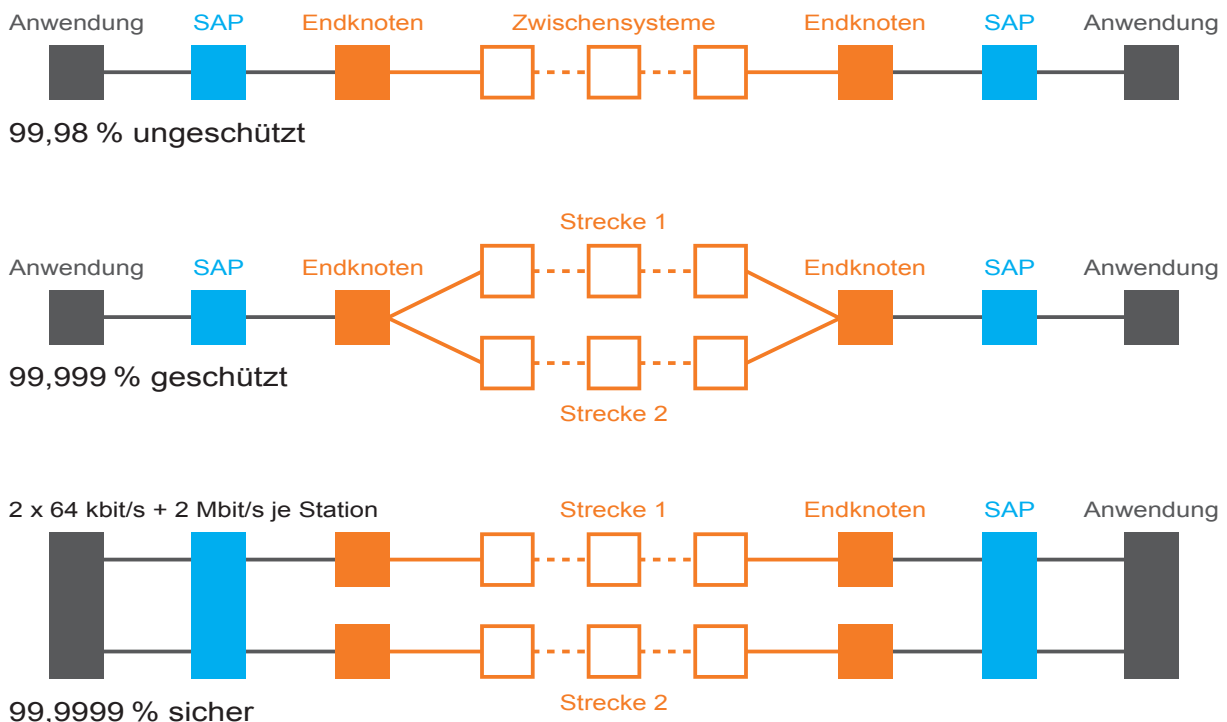
Redundant sind alle Betriebsmittel, die es nicht brauchen würde, wenn es keine Fehler gäbe. Wir betrachten weiter Systeme, bei denen die Redundanz automatisch eingefügt wird sowie Systeme, bei denen die Redundanz nach der

Reparatur nahtlos eingefügt werden kann (unterbrechungsfreie Systeme).

Ein entsprechendes Übertragungsnetz lässt sich dabei in drei Klassen bezüglich seiner Verfügbarkeit z. B. in Minuten pro Jahr bzw. in Prozent wie folgt darstellen:

- 99,98 % ungeschützt  
(ca. 1,75 Stunden pro Jahr nicht erreichbar)
- 99,999 % geschützt  
(ca. 5 Minuten pro Jahr nicht erreichbar)
- 99,9999 % sicher  
(ca. 32 Sekunden pro Jahr nicht erreichbar)

Je nach Verfügbarkeitsgrad kann die Bahnanwendung einfach- oder doppelredundant an den Übertragungsknoten (SAP, Single Access Point) angebunden werden.



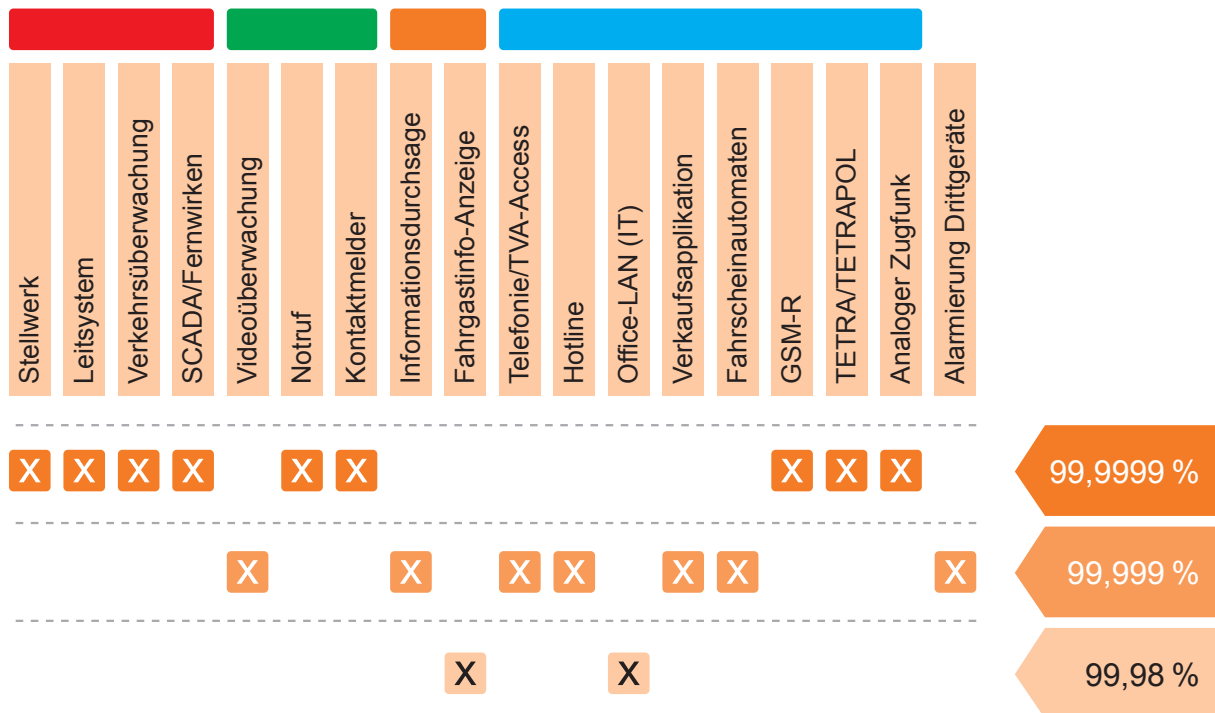
Grafik 3: Verfügbarkeitskategorien

Gleichzeitig können anhand der Prozentangaben, die sich aus den Zuverlässigkeitszahlen der Einzelelemente (MTTF) für die gesamte Netztopologie errechnen lassen, die Wahrscheinlichkeit dafür ablesen, dass ein Gesamtsystem auch tatsächlich die angegebene Leistung erbringt.

Ob nun Systeme und ihre Einzelkomponenten einfach oder gar doppeltredundant eingesetzt werden müssen, hängt im Wesentlichen vom Verfügbarkeitsgrad der Bahnanwendung ab.

Hier eine Zusammenstellung der häufigsten Bahnanwendungen, gegliedert nach deren Verfügbarkeitsanforderung.

Zu bemerken ist, dass eine noch so ausgeklügelte Redundanz kein Ersatz für Qualität der eingesetzten Systemkomponenten der Übertragungstechnik sein kann.



Grafik 4: Ausfallwahrscheinlichkeit nach einzelnen Bahnanwendungen

### 3.3. Die Grenzen der Redundanz

Dank Redundanz und Fehlertoleranz hängt die Verfügbarkeit nur noch von der Wahrscheinlichkeit eines zweiten Ausfalles ab, bevor der erste repariert ist. Die Verfügbarkeit steigt jedoch demgemäß nicht ins Unendliche.

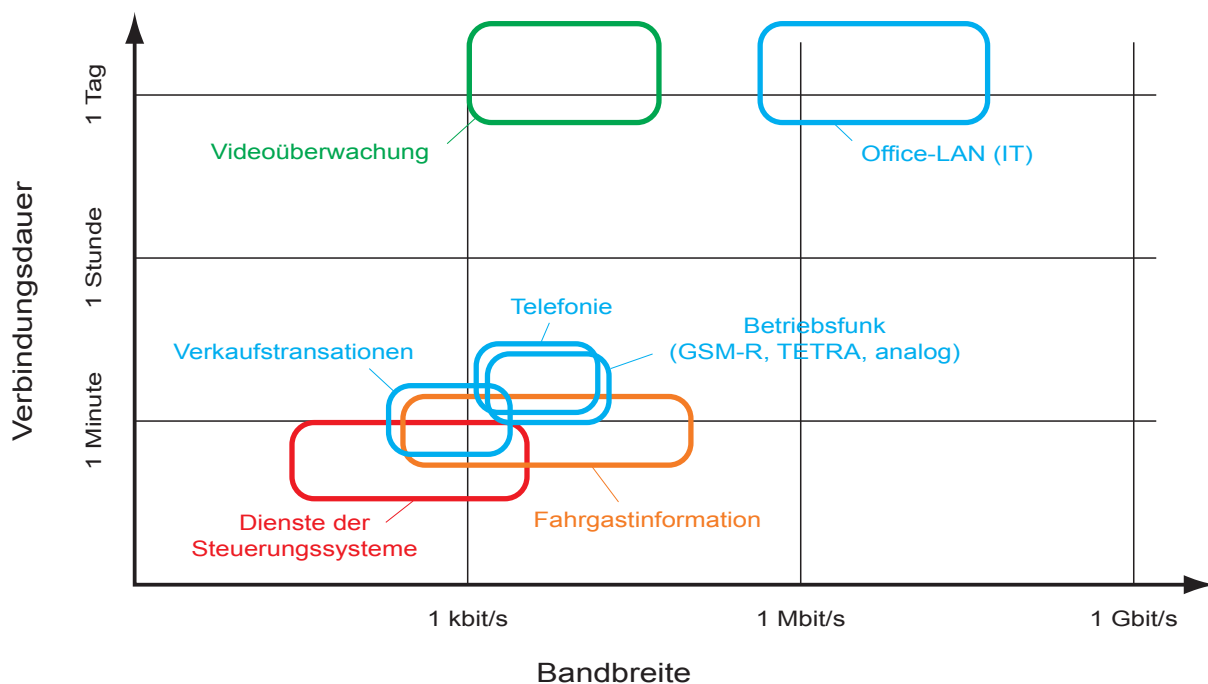
Das einzig Sichere bei einem doppeltredundanten System ist, dass es mehr als doppelt so teuer ist und mehr als doppelt so oft ausfällt. Darum sollte man sich über die Zuverlässigkeit und Verfügbarkeitsziele im Klaren sein, bevor redundante Lösungen betrachtet werden.

## 4. Trends im Bahnen-Sektor

### 4.1. Steigender Bandbreitenbedarf

Die heterogene Netztechnik von Systemen der Leit- und Sicherungstechnik ist jahrzehntelang gewachsen. Sie steht heute unter dem Druck von Modernisierung und damit einhergehender Kostensenkung und Leistungssteigerung. Signaltechnische Anwendungen übertragen in der Regel mehrere Größenordnungen weniger Datenvolumen als die technikbestimmenden anderen IT-Anwendungen. Dennoch ergibt sich

auch in der Leit- und Sicherungstechnik durch steigende Anforderungen an Flexibilität und Leistungsausweitung der Leit- und Bediensysteme, des Systemmanagements, der (Fern-) Diagnose, der Wartungsdienste usw. ein kontinuierlicher Anstieg des Bedarfs an Datenübertragungskapazität.



Grafik 5: Bandbreitenbedarf der einzelnen Bahnanwendungen

Die Zeit, in der ein 64-kbit/s-Kanal wie bisher zwischen zwei Standorten in allen Fällen ausreicht, wird bald zu Ende gehen. Denn bisher noch getrennt übertragene Kommunikationsbeziehungen, neu hinzukommende Fernübertragungen (z. B. Radio Block Center von den Betriebszentralen aus) oder ganz neue Dienste (etwa Wartungsdienstzentralen) werden zukünftig kostensparend über gemeinsame Netzverbindungen geschaltet werden. Über kurz oder lang dürften im Bereich eines großen Betreibers die WAN-Verbindungen mit 2 Mbit/s zumindest zwischen großen Knoten wie Betriebszentralen und Unterzentralen die Regel werden; damit wäre auch genügend

Bandbreite vorhanden, um bei steigender Datenlast die Echtzeitanforderungen für zeitkritische Anwendungen noch eine Zeit lang mit den derzeitigen TCP/IP-Basisprotokollen zu erfüllen, bei gleichzeitiger Reserve für weitere Anwendungen.

Ansonsten müssten am Engpass eines 64-kbit/s-Kanals prioritätssteuernde Zusatzprotokolle mit der Konsequenz von Verzögerungszeiten für nachrangige Anwendungen eingesetzt werden.

## 4.2. Leistungsfähige Netzinfrastruktur

Aus dem Blickwinkel der Leit- und Sicherungstechnik sind vor allem zwei Evolutionsrichtungen zu erkennen. Die eine ist die Entwicklung hin zu Netze- und Dienstintegrierenden Großsystemen (man spricht auch von „konvergierenden Netzen“). Zum anderen ist es die zunehmende Anwendung von Verfahren zur Sicherung geschlossener Teilnetze innerhalb von Großnetzen („Network Security“).

Dienstintegrierende Systeme bedeutet unter anderem, dass auch Echtzeitdienste wie Sprach- und Live-Videodienste über IP-Netze übertragen werden, die heute noch eher für zeitunkritische Rechnerdatenkommunikation ausgelegt sind. Ebenso sollen auch Dienste der Sicherheits- und Leittechnik (z. B. Rail-IP) übertragen werden.

Die dafür heute gebräuchliche TCP/IP-Protokoll-Familie, zu der auch das unter Lastbedingungen schneller übertragende, dafür aber nicht gegen Übertragungsfehler schützende Protokoll UDP gehört, bietet noch keine befriedigenden Möglichkeiten, um bei Bedarf unter allen Umständen kurze Durchlaufzeiten und fehlerfreie Übertragung zu garantieren. So müssen im Unterbrechungsfall Konvergenzzeiten von wenigen „ms“ (typ. 50 ms) auf die Rückfallebene eingehalten werden.

Für die Leit- und Sicherungstechnik sind die Merkmale der Dienstgüte (Quality of Service, QoS) und schnelle Konvergenzzeiten wichtig. Die Standardlösungen aus dem Metro-Ethernet-IP-Umfeld erfüllen heute noch nicht die Anforderung für ihre Verwendung im Bereich der Leit- und Sicherungstechnik. Dennoch bieten diese Technologien unbestritten Potenzial im Hinblick auf die Datenübertragungskapazität. Deshalb werden heute zwei Wege bestritten. So steht eine Erweiterung der IP-Transport-Grundfunktionen um ein Protokoll namens Multi-Protocol Label Switching (MPLS) an. Bei der MPLS-Technologie wird dem IP-Datenpaketen während des Transports im Datennetz eine zusätzliche Kennzeichnung (Label) angehängt.

Anhand dieser Information beachten MPLS-fähige Router unterschiedliche Prioritäten und Dienstklassen der einzelnen Datenpakete und weisen ihnen je nach deren Dienstklasse qualitativ unterschiedliche Wege durch das Datennetz zu. MPLS gilt in Bezug auf das Konfigurationsmanagement als sehr aufwendig und wird dadurch im Betrieb und Unterhalt als komplex angesehen.

Ein weiteres Verfahren namens „Next Generation SDH“ (NG-SDH) setzt auf die bewährte TDM-basierte SDH-Infrastruktur mittels Ethernet over SDH (EoS) auf. Mit Ethernet over SDH wird die paketoptimierte Ethernet-Technik mit dem echtzeitoptimierten TDM-Verfahren von der Synchronous Digital Hierarchy (SDH) kombiniert. In der Kombination beider Techniken werden die Vorteile genutzt und deren Nachteile verhindert. Die Realisierung der EoS-Technik umfasst ein flexibles Bandbreitenmanagement mit dynamischer Bandbreitenzuordnung an den Kommunikationsbedarf, die physikalische Netztrennung, den verzögerungsfreien Datentransport sowie die Integration der Ethernet-Schnittstellen in SDH.

EoS bietet für Netzbetreiber eine interessante Alternative zu MPLS, zumal ein Echtzeitverhalten vorliegt und die Dienstgüte (QoS) angepasst werden kann. Im Weiteren erlaubt NG-SDH die Konsolidierung aller Dienste auf ein einziges, höchstverfügbares Datennetz.

Weitere Protokolle, wie Provider Backbone Transport (PBT), sollen die spezifischen Randbedingung wie oben erwähnt ebenfalls berücksichtigen. Sie werden von namhaften Herstellern vorangetrieben, sind allerdings noch nicht feldtauglich geprüft.

Die unten aufgeführte Darstellung fasst nochmals die Eigenschaften der verschiedenen Übertragungstechnologien zusammen.

	Reife	TDM Support	Schutzmechanismen und -leistung	Konfiguration	Betrieb und Unterhalt
NG-SDH	SDH ~ 15 Jahre NG-SDH ~ 5 Jahre	nativ	Path- und Section-Protection (vorkonfiguriert) <50 ms	ausgereift, einfach	viele Funktionen, effizient
METRO ETHERNET	~ 1 bis 3 Jahre	Emulation	Spanning Tree, Ethernet Protection, Switching, Link Aggregation <50 ms	wenig Funktionen, kein „End-to-End“	OAM-Standardisierung in Abschlussphase
MPLS (IP)	~ 6 Jahre	Emulation	alternative Routen (vorkonfiguriert) <50 ms	aufwendiges Traffic-Engineering	hohe Komplexität
PBT	noch keine Felderfahrung, Technologie zu neu	Emulation	alternative Routen (vorkonfiguriert) <50 ms	ähnliche Funktionen wie bei SDH	noch keine Felderfahrung, Technologie zu neu

Grafik 6: Eigenschaften der verschiedenen Übertragungstechnologien

Die Entwicklungen der unterschiedlichen Übertragungstechnologien waren bisher auch von der Annahme einer sehr starken Zunahme des Bedarfs an Übertragungskapazität getrieben. Die Hierarchiestufen der eingeführten SDH-Technik reichen von 155 Mbit/s bis 10 Gbit/s, und die teilweise schon realisierte und weiter anvisierten optischen Netze mit fortgeschrittener Wellenlängen-Multiplex-technologie gehen bis 40 Gbit/s und zukünftig wohl auch darüber hinaus.

Mit dem Einzug der Local Area Network (LAN)-Technologie steht der Leit- und Sicherungstechnik die bereits installierte SDH-Basis im Transportnetz zu Verfügung.

Mit EoS-fähigen Netzkomponenten werden SDH-Systeme NG-SDH-fähig. Damit lassen sich Ethernet-basierte Dienste der Leit- und Sicherungstechnik sicher übertragen. Die Übertragungsleistung von anfangs 10 Mbit/s auf inzwischen standardmäßige 100 Mbit/s bis zu vielfach schon üblichen 1 Gbit/s stellen dabei kein Problem dar.

Ebenso ist es auch möglich, die herkömmliche Zweidraht-Kupferleitung mittels symmetrischer DSL-Technologie mit  $n \times 5,7$  Mbit/s in TC-PAM 32 Ethernet-Dienste mit bis zu 100 Mbit/s zu übertragen.

## 5. Schlussfolgerung

Die Datenkommunikation der Leit- und Sicherungstechnik bleibt aus der Sicht der Informations- und Telekommunikationstechnik ein Sonderfall in Bezug auf

- heute noch relativ niedrige Datenraten,
- besonders hohe Sicherheitsanforderungen und
- relativ lange Innovationszyklen der Nutzersysteme.

Die grundsätzlichen Entwicklungsrichtungen der Informations- und Telekommunikationstechnik finden sich jedoch zwangsläufig auch in der Anwendung der Leit- und Sicherungstechnik wieder, was derzeit in der Ausbreitung von moderner LAN/WAN-Technik im Übergang zu IP zu verfolgen ist.

Im Detail befinden sich die Netz-Designer der Leit- und Sicherungstechnik im Spannungsfeld zwischen Kompatibilität mit den Bestandssystemen, national unterschiedlichen Anforderungen der Bahnbetreiber an neue Lösungen, internationalen Standardisierungstendenzen in der

Leit- und Sicherungstechnik sowie kostengünstigen, aber nie genau passenden Standardlösungen des Weltmarkts der Informations- und Telekommunikationstechnik.

In Anbetracht der unterschiedlich langen Innovationszyklen besteht immer das Problem, zu entscheiden, wann ein neuer Trend der allgemeinen Informations- und Telekommunikationstechnik als beständig und zukunftsbestimmend erkannt wird, so dass die Übernahme in die Leit- und Sicherungstechnik mit ihren länger dauernden Erprobungs- und Zulassungsprozessen wirtschaftlich ist.

Am Ende müssen die Netze so konzipiert werden, dass sie als zulassungsfähiges Gesamtsystem für die Leit- und Sicherungstechnik realisiert werden können. Daher setzt KEYMILE bei seinen Bahnkunden weltweit auf sein ganzheitliches und zukunftsweisendes Multi-Service Zugangssystem UMUX.

Herausgeber  
KEYMILE GmbH  
Wohlenbergstraße 3  
30179 Hannover, Deutschland

Telefon +49 511 6747-0  
Fax +49 511 6747-450  
Internet [www.keymile.com](http://www.keymile.com)  
Mail [info@keymile.com](mailto:info@keymile.com)