**Zeitschrift:** Bulletin Electrosuisse
**Herausgeber:** Electrosuisse, Verband für Elektro-, Energie- und Informationstechnik
**Band:** 99 (2008)
**Heft:** 6

**Artikel:** Damit wir nicht im Dunkeln tappen
**Autor:** Willisegger, Jonas
**DOI:** https://doi.org/10.5169/seals-855836

# Damit wir nicht im Dunkeln tappen

## ICT-Risikoanalyse in der Elektrizitätsbranche

**Die rasante Entwicklung der Informations- und Kommunikationstechnologien (IKT bzw. ICT) steigert die wirtschaftliche Produktivität und eröffnet neue Möglichkeiten im Energiesektor. Allerdings entstehen durch die technologischen Fortschritte zahlreiche Abhängigkeiten und damit neue Herausforderungen und Risiken für die Stromversorgung. So kann ein Ausfall oder eine Störung der ICT-Infrastruktur zu weitreichenden Strompannen führen. Vertreter von Firmen, Branchenverbänden und Behörden analysierten im Rahmen der wirtschaftlichen Landesversorgung die ICT-Infrastrukturen der Elektrizitätsbranche und entwickelten gemeinsam präventive Massnahmen für den sicheren Einsatz der ICT bei der Stromversorgung.**



*Jonas Willisegger*

ICT-Anwendungen durchdringen im Zuge des technischen Fortschritts sämtliche Wirtschaftszweige. Auch die Elektrizitätsbranche verlässt sich bei ihrer Kernaufgabe – der sicheren Stromversorgung – auf komplexe ICT-Systeme. Insbesondere im Bereich des Störungsmanagements ist der Netzbetrieb auf eine einwandfrei funktionierende ICT-Infrastruktur angewiesen.

Die zunehmende «Informatisierung» der Elektrizitätsbranche hat nicht nur wachsende Abhängigkeiten von der ICT-Infrastruktur und den damit verbundenen Dienstleistungen, sondern auch neue Risiken zur Folge. Die dichte Vernetzung von Kommunikationssystemen erhöht beispielsweise die Angriffsfläche für Hackerangriffe und schädliche Software wie Viren, Würmer und trojanische Pferde. Diese können sich in kürzester Zeit über Netzwerke verteilen und Geschäftsprozesse lahmlegen. Aber auch menschliches Fehlverhalten, unzureichende Hard- und Software sowie Inkompatibilitäten zwischen verwendeten Technologien können zu Störungen führen. In solchen Fällen ist die Stromversorgung ernsthaft gefährdet.

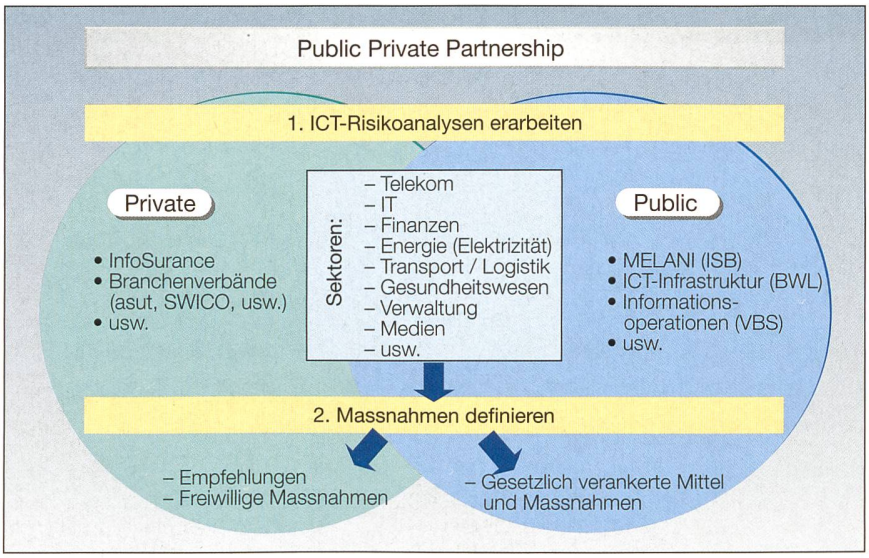


**Bild 1 Zusammenarbeit zwischen Privatwirtschaft und staatlichen Stellen bei der Erarbeitung von Risikoanalysen und der Formulierung präventiver Massnahmen.**

### Public Private Partnership zwischen Bund und Wirtschaftssektoren

Als Reaktion auf die drohenden ICT-Risiken und im Hinblick auf eine sichere Versorgung unseres Landes mit lebenswichtigen Gütern und Dienstleistungen haben Wirtschaft und Behörden im Sinne des Public Private Partnership gemeinsam das Konzept «Information Assurance Schweiz» erarbeitet, welches im Jahr 2000 vom Bundesrat genehmigt wurde. Im Zentrum dieses Konzepts zum Schutz kritischer ICT-Infrastrukturen stehen die Prävention, die Früherkennung, das Krisenmanagement und die Behebung von ICT-Störungen.

Seit 2004 bietet die wirtschaftliche Landesversorgung im Rahmen der Prävention für die unterschiedlichsten Sektoren und Branchen eine Plattform zur Erarbeitung von Risikoanalysen und daraus abgeleiteten präventiven Massnahmen auf dem Gebiet der ICT-Sicherheit an. Solche Risikoanalysen sind inzwischen für die Sektoren Telekommunikation, Informationstechnologie (Hard- und Software), Finanzen, Gesundheitswesen (Spitäler und Arztpraxen), Transport- und Logistikleistungen sowie Energie (Elektrizität) erstellt worden. Die Analysen werden unter der Leitung des Bundesamtes für wirtschaftliche Landesversorgung (BWL) nach einer einheitlichen Methode durchgeführt, sodass die Ergebnisse zwischen den einzelnen Sektoren ausgetauscht und miteinander verglichen werden können. Damit profitieren alle beteiligten Sektoren von einem übergreifenden Netzwerk in den Bereichen Prävention und Krisenbewältigung.

Im Sektor Energie haben sich die für die Sicherheit verantwortlichen Vertreter der Elektrizitätsbranche (Swissgrid, EGL AG, EOS Holding, EWZ, Axpo, NOK, KKW Gösgen, Atel usw.) und staatliche Stellen (Bundesamt für Energie und BWL) als Arbeitsgruppe an der Risikoanalyse beteiligt. Dabei wurde der Fokus auf die Relevanz der ICT-Infrastruktur für die Stromversorgung gerichtet.

### Die Kernleistungen der Elektrizitätsbranche

Zunächst identifizierte die Arbeitsgruppe die Kernleistungen der Elektrizitätswirtschaft. Dazu gehören Stromproduktion,

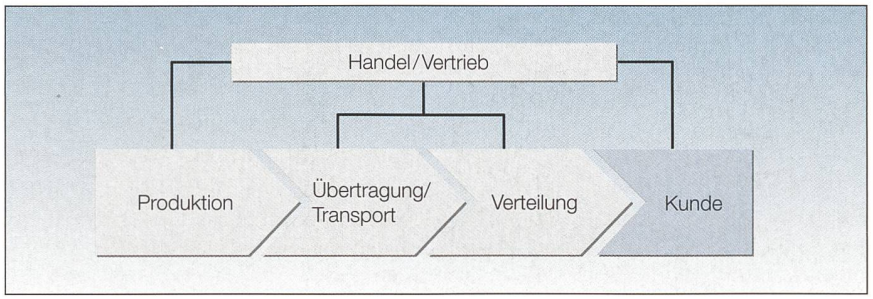


**Bild 2 Kernleistungen der Elektrizitätswirtschaft.**

Übertragung/Transport, Verteilung und Handel/Vertrieb (Planung der Energiebeschaffung und des Absatzes).

Die Übertragungs- und Verteilungsnetze stellen auch in einem liberalisierten Strommarkt ein natürliches Monopol dar und müssen allen Marktteilnehmern diskriminierungsfrei zur Verfügung stehen. Eine Störung in einem Verteilnetz (z.B. durch Kurzschluss in einem Verteiltrafo) hat einen Stromausfall bei den angeschlossenen Endkunden zur Folge. Die Auswirkungen eines solchen Ausfalls sind in der Regel lokal. Grossräumige Stromausfälle ereignen sich insbesondere bei Störungen im Übertragungsnetz, weil alle darunter liegenden Verteilnetze betroffen sind.

## Relevanz der ICT-Infrastruktur für die Stromversorgung

Im Rahmen der Risikoanalyse in der Elektrizitätsbranche hat die Arbeitsgruppe eine ICT-Störung wie folgt definiert: Stromausfall bei mindestens 10000 Kunden (Anschlüssen) während einer Mindestdauer von 4 Stunden. Ausfälle dieser Grössenordnung sind in der Schweiz selten. Zudem besitzt die Stromversorgung die charakteristische Eigenschaft, dass im Normalbetrieb keine übergeordnete, aktive Stabilisierung notwendig ist. Im normalen Betriebszustand führt also eine ICT-Störung von weniger als 2 bis 3 Stunden selbst wichtiger Informatikmittel nicht zu einem Stromausfall.

Allerdings wird die ICT-Infrastruktur zu einem entscheidenden Faktor, wenn sich der Netzbetrieb ausserhalb des Normalzustands befindet (z.B. bei plötzlichem Wegfall grosser Kraftwerke, bei Betriebssituationen nahe an der Stabilitätsgrenze, bei grossen Unwettern usw.). In kritischen Situationen sind wenige Minuten entscheidend, ob es zu einem Stromausfall kommt. ICT-Systeme liefern in diesem Zusammenhang wichtige Daten als Entscheidungsgrundlage. Stehen sie in kritischen Momenten nicht zur Verfügung, besteht ein hohes Risiko für Stromausfälle. Deshalb wurde in der Risikoanalyse nicht vom Normalbetrieb ausgegangen, um die Relevanz von ICT-Störungen abschätzen zu können, sondern von einem kritischen Zustand, bei dem eine aktive Stabilisierung mittels ICT-Infrastruktur notwendig ist. Somit besteht für die Stromversorgung dann eine Schwachstelle, wenn eine Netzstörung aufgrund von nicht funktionierender oder fehlerhafter ICT-Infrastruktur nicht gehandhabt werden kann.

## Abhängigkeiten und Schwachstellen der Stromversorgung

Die Analyse der Abhängigkeiten kam zu folgendem Schluss: Kritische Prozesse befinden sich vorwiegend im Bereich Übertragung und Verteilung, weil gerade dort äusserst wichtige ICT-Ressourcen für die Netzführung und das Transportmanagement eingesetzt werden. Für die meisten Prozessausfälle existieren zwar Umgehungslösungen manueller Natur. Diese erfordern aber eine funktionsfähige Kommunikationsinfrastruktur (Telefon, Fax, E-Mail usw.).

Im Gegensatz zur Übertragung und Verteilung wurde die Stromproduktion nicht als eine versorgungskritische Kernleistung bezeichnet, weil der Ausfall eines einzelnen Kraftwerks in der Regel keinen Stromausfall bei Konsumenten zur Folge hat. Zudem kommen Kraftwerksausfälle relativ häufig vor.

Basierend auf den analysierten Abhängigkeiten wurden Schwachstellen der Stromversorgung im Zusammenhang mit der eingesetzten ICT-Infrastruktur identifiziert. Dazu gehört unter anderem die zunehmende Zentralisierung der Übertragungs- und Verteilnetzbetreiber als Folge des erhöhten Kostendrucks und neuer technischer Möglichkeiten. Mit der Zentralisierung steigen die Anforderungen an die Verfügbarkeit und Zuverlässigkeit der ICT-Infrastruktur bei den zentralen Leitstellen. Redundanzen beim Personal und bei der Infrastruktur fallen damit weg. Eine weitere Schwachstelle stellt die zunehmende Entfernung zwischen Produktion und Verbrauch dar. Daraus ergeben sich hohe physische Netzflüsse mit entsprechender Belastung der Übertragungsnetze. Dies erhöht die Wahrscheinlichkeit eines Zustands ausserhalb des Normalbetriebs und damit die Abhängigkeit von der ICT-Infrastruktur.

## Analyse der Risiken für die Stromversorgung

Zur vertieften Untersuchung der identifizierten Schwachstellen und deren Auswirkungen im Krisenfall wurde für die Risiko-

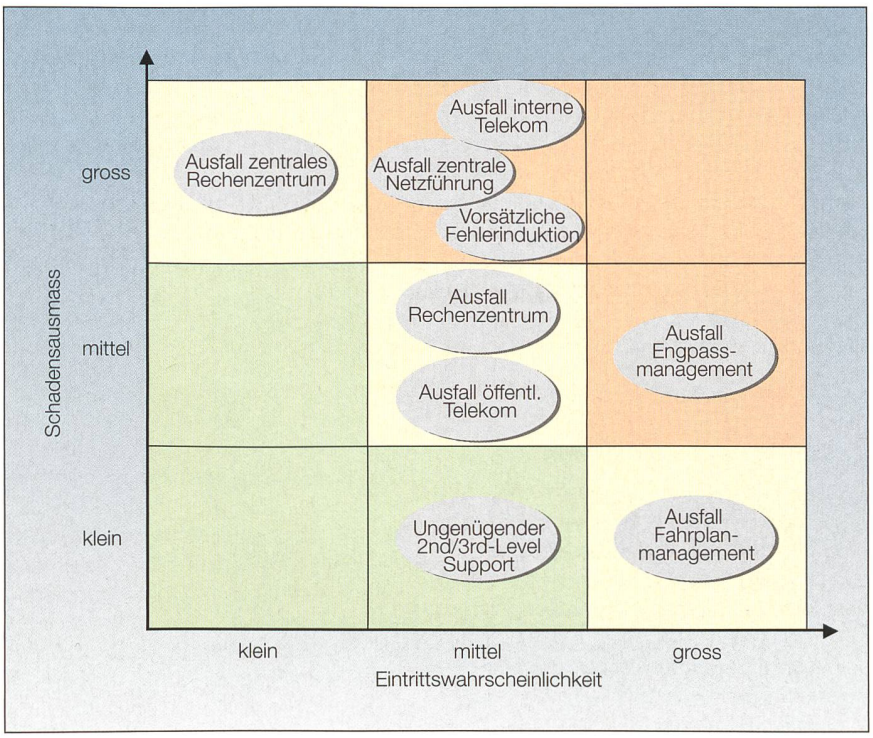


**Bild 3 Risikomatrix mit neun ausgewählten Szenarien.**

analyse der Stromversorgung die Szenariotechnik verwendet. Die Arbeitsgruppe analysierte das Schadensausmass und die Eintrittswahrscheinlichkeit von 15 Szenarien, welche potenzielle Schadensereignisse beschreiben.

Zu den Szenarien, die untersucht wurden, gehört beispielsweise der Ausfall des zentralen Fahrplanmanagementsystems bei Swissgrid durch fehlerhafte Hard- oder Software oder durch eine Fehlmanipulation. In diesem Fall wird die Fahrplanabstimmung schweizweit und im benachbarten Ausland erschwert, was zu einem substanziellen Mehraufwand (Notbetrieb, telefonische Abstimmung usw.), zu einer erhöhten Fehlerquote in der Netzführung und möglicherweise zu finanziellen Einbussen für einzelne Marktteilnehmer führt.

Als weiteres Szenario wurde der Ausfall eines Telekomanbieters betrachtet, was beispielsweise den Support wichtiger Systemkomponenten (Hard- und Software) durch Lieferanten behindern kann. So wäre etwa die Auslieferung eines Patches zur Schliessung elektronischer Sicherheitslücken im Betriebssystem bei einer Telekomstörung erschwert.

Des Weiteren wurde die vorsätzliche Fehlerinduktion bei ICT-Systemen durch Hacking, Social Engineering, Viren, Würmer, trojanische Pferde usw. analysiert. Zudem zählen Ausfälle und Störungen des Engpassmanagements, des Rechenzentrums von Swissgrid, des zentralen Netzführungssystems und der internen Telekommunikation (LAN/MAN/WAN) zu den Bedrohungen für die Stromversorgung.

Die Arbeitsgruppe orientierte sich bei der Risikoeinschätzung für die untersuchten Szenarien an Abschätzungen aus historischen Netzstörungen. Dabei zeigte sich deutlich, dass die Szenarien, bei denen die grössten Schäden zu erwarten sind, vor allem im Bereich der Übertragungsnetze auftreten und mit der zunehmenden Zentralisierung des Netzbetriebs zusammenhängen. Störungen in einem zentralisierten System betreffen nicht mehr bloss einzelne Bilanzzonen, sondern wirken sich flächendeckend auf die gesamte Schweizer Stromversorgung aus.

## Empfohlene Massnahmen

Basierend auf der Risikoanalyse hat die Arbeitsgruppe diverse Präventivmassnahmen für die Elektrizitätsbranche festgelegt und Swissgrid, den Übertragungsnetz-Eigentümern und Verteilnetzbetreibern empfohlen.

Die Liste der Empfehlungen umfasst einerseits branchenunabhängige Massnahmen, deren Umsetzung in jedem Unternehmen präventiv zur ICT-Sicherheit beiträgt. Dazu gehört etwa der Aufbau eines firmenübergreifenden Business Continuity Managements (BCM). BCM bezieht sich auf die Sicherstellung der Verfügbarkeit von kritischen Geschäftsprozessen eines Unternehmens, die bei Ausfällen von Ressourcen aufrecht erhalten bleiben müssen. Demzufolge wird den Netzbetreibern empfohlen, ihre betriebsspezifischen Risiken zu analysieren, ihre Rechenzentren und Kommunikationssysteme redundant auszulegen, die Systemarchitekturen aufeinander abzustimmen, Notfallkonzepte zu erarbeiten und aktuelle ICT-Sicherheitstechnologien (Virenschutz, Patchmanagement, Firewall, Intrusion-Detection-Systeme, Identity Management usw.) einzusetzen und zu koordinieren. Zudem sollten Mitarbeitende der Energieversorgungsunternehmen auf wichtige Punkte der ICT-Sicherheit sensibilisiert und entsprechend geschult werden.

Andererseits beinhalten die Empfehlungen Massnahmen, die auf die charakteristische Risikostruktur der Stromversorgung ausgerichtet sind. So werden die Branchenverbände dazu angeregt, Standards für sektorspezifische Sicherheitsthemen zu erarbeiten. Von zentraler Bedeutung für Stromnetzbetreiber sind klare Vorgaben über Aufbau und Einsatz der Sprachkommunikationsinfrastruktur (Notfallverbindungen, Ausweichmöglichkeiten) sowie über die Verantwortlichkeiten bei kritischen Systemen (Leittechnik, Engpassmanagement, Fahrplanmanagement usw.).

Der VSE hat bereits auf die Empfehlungen reagiert und konkrete Massnahmen ausgearbeitet. So wird der Schlussbericht der ICT-Risikoanalyse auf der Internetseite des VSE als Download zur Verfügung stehen. Zudem plant der VSE, ein Branchenhandbuch zur ICT-Sicherheit für die Bedürfnisse der kommunalen und kantonalen Elektrizitätswerke zu entwickeln und branchenspezifische Schulungen für Sicherheitsverantwortliche anzubieten.

## Sektorübergreifende Zusammenarbeit notwendig

Die eingangs erwähnten Wirtschaftssektoren, in denen bereits ICT-Risikoanalysen durchgeführt wurden, sind dabei, ihre Ergebnisse gegenseitig auszutauschen. Die sektorübergreifende Zusammenarbeit wird von den Verantwortlichen als ein wesentlicher Vorteil erkannt, denn die Abhängigkeiten zwischen den Sektoren sind offensichtlich und wurden auch in der Risikoanalyse der Elektrizitätsbranche augenfällig: Eine stabile Stromversorgung hängt unmittelbar von der einwandfrei funktionierenden Telekommunikation und IT (Hard- und Software) ab. Die Bereitschaft zur Kooperation über die eigene Branche hinaus erhöht folglich die Sicherheit der Kernprozesse in allen Sektoren und damit die wirtschaftliche Versorgungsstabilität unseres Landes.

## Links

[1] Information Assurance Schweiz: www.melani.admin.ch; www.infosurance.ch; www.bwl.admin.ch
[2] Business Continuity Management: www.bcmnet.ch

## Angaben zum Autor

*Jonas Willisegger*, Politologe (lic. rer. soc.), arbeitet als wissenschaftlicher Mitarbeiter für die Geschäftsstellen Infrastruktur und Grundversorgung des Bundesamtes für wirtschaftliche Landesversorgung. Er organisiert und betreut die Zusammenarbeit zwischen Privatwirtschaft und Behörden bei der Erstellung von Risikoanalysen und Massnahmeplänen, erarbeitet Grundlagen zu Business Continuity Management und beteiligt sich an der internationalen Zusammenarbeit mit dem Civil Emergency Planning (NATO) im Bereich der zivilen Kommunikationsinfrastrukturen.
*Bundesamt für wirtschaftliche Landesversorgung, jonas.willisegger@bwl.admin.ch.*

*Résumé*

**Pour éviter les mauvaises surprises…**

*Analyse des risques ICT dans la branche de l'électricité.* L'évolution fulgurante des technologies de l'information et de la communication (TIC, ou ICT en anglais) permet d'augmenter la productivité des entreprises et ouvre des perspectives nouvelles pour le secteur de l'énergie. En même temps, le progrès technologique engendre aussi de nombreuses interdépendances, ce qui est synonyme de nouveaux défis et risques pour l'approvisionnement en électricité. Ainsi, une panne ou une perturbation des infrastructures ICT peut par exemple engendrer des pannes de courant importantes. Des représentants des entreprises, des associations de branche et des autorités se sont réunis pour analyser les infrastructures ICT de la branche électrique du point de vue de l'approvisionnement économique du pays, et ils ont élaboré des mesures préventives visant à une sécurité maximale dans l'exploitation des infrastructures ICT liées à l'approvisionnement en électricité.

# Arbeitsschutzgesetz verpflichtet

## Gebrauch und Instandhaltung von isolierenden Stangen

**Jeder Unternehmer trägt für Sicherheit und den Gesundheitsschutz in seinem Unternehmen die Gesamtverantwortung. So ist er entsprechend dem Arbeitsschutzgesetz verpflichtet darauf zu achten, dass beim Arbeiten an elektrischen Anlagen alle notwendigen Schutzmaßnahmen getroffen und auch eingehalten werden.**

Deshalb werden bei Arbeiten an elektrischen Anlagen und Betriebsmitteln die betreffenden Anlagenteile spannungsfrei geschaltet. Doch die simple Betätigung eines Schalters zur Freischaltung reicht bei weitem nicht aus. Eine gesicherte Aussage zur Spannungsfreiheit und damit zum Ausschluss des Gefahrenpotentials der Elektroenergie lässt sich damit nicht treffen. Von der Freischaltung einer Anlage bis zur Freigabe der Arbeitsstelle bedarf es weiterer sicherer Informationen und Maßnahmen. Dazu wurden die fünf Sicherheitsregeln formuliert:

- *Freischalten*
- *Gegen Wiedereinschalten sichern*
- *Spannungsfreiheit feststellen*
- *Erden und Kurzschließen*
- *Benachbarte, unter Spannung stehende Teile abdecken oder abschranken*

Jeder Elektrofachkraft sind diese Regeln als ihre Lebensversicherung wohl bekannt. Doch wie steht es um die Sicherheit und Verlässlichkeit der Geräte und Hilfsmittel mit denen sie ihre lebenswichtigen Informationen gewinnen oder Arbeitsabläufe absichern muss? Jede Maßnahme ist nur so sicher, wie die dazu benutzten Technologien.

Zum Herstellen des spannungsfreien Betriebszustandes wird in Mittel- und Hochspannungsanlagen das Arbeitsverfahren „Arbeiten auf Abstand" mit isolierenden Stangen eingesetzt. Beim „Arbeiten auf Abstand" bleibt der Monteur in einem festgelegten Abstand zu unter Spannung stehenden Anlagenteilen und führt die Arbeiten mit isolierenden Stangen aus (z. B. Freischalten, Prüfen auf Spannungsfreiheit, Erden und Kurzschließen). Doch auch diese Sicherheitsmaßnahme ist nur so gut, wie die dazu verwendeten Mittel. Das heißt, die Geräte müssen dem Verwendungszweck entsprechen, richtig bemessen und entsprechend der Gebrauchsanweisung angebracht sein und sich in einem ordnungsgemäßen Zustand befinden. Ein beschädigtes Isolierteil oder eine nicht richtig ausgewählte isolierende Stange kann beim Eintauchen in die Gefahrenzone oder beim Berühren unter Spannung stehender Anlageteile zu Ableitstromerhöhungen führen. Dies kann im Extremfall eine tödliche Körperdurchströmung für den Monteur bedeuten. Ein defektes Verlängerungsteil oder Metallteile im Bereich des Arbeitskopfes von isolierenden Stangen können beim Eintauchen in enge Bereiche der Anlage zu Überschlägen und zur Zündung von folgenschweren Störlichtbögen führen. Schutz- und Hilfsmittel müssen mit einem normgerechten Typenschild versehen sein. Sie dürfen nur für Anlagen verwendet werden, für die sie entsprechend dem Typenschild ausgelegt sind. Ohne Typenschild, Herstellerkennung, Nennspannungs-/Nennspannungsbereichsangabe, Doppeldreieck mit Normenbezug oder Doppelisolator sind Schutz- und Hilfsmittel der Weiterverwendung zu entziehen. Isolierende Stangen sind Schutz- und Hilfsmittel, für die Prüffristen und die Art der Prüfungen festgelegt sind. Die Frist für eine Wiederholungsprüfung richtet sich nach Einsatzbedingungen wie:

- *Häufigkeit der Benutzung*
- *Beanspruchung durch Umgebungsbedingungen und Transport*

Für kapazitive Spannungsprüfer ist nach BGV A3 eine Wiederholungsprüfung mindestens alle 6 Jahre gefordert.

Der Unternehmer hat dafür zu sorgen, dass Schutz- und Hilfsmittel vor jeder Anwendung auf ihren ordnungsgemäßen Zustand und in bestimmten Zeitabständen auf die Einhaltung der in den elektrotechnischen Regeln vorgegebenen Grenzwerte geprüft werden. Die Fristen sind so zu bemessen, dass entstehende Mängel, mit denen gerechnet werden muss, rechtzeitig erkannt werden.



**Für Wiederholungsprüfungen an Spannungsprüfern, Schaltstagen, Sicherungszangen, Isolierstangen und Erdungsstagen stehen wir Ihnen gerne als verlässlicher Partner zur Seite.**