

HANDBUCH BLACKOUT



Vorbereitung zur Führung von Einsätzen
ohne
Netzstrom - Computer - Telefon

Zivilschutz
Katastrophenschutz



tirol
Unser Land

NUR für den INTERNEN Gebrauch



Vorwort

LH-Stv. ÖR Anton Steixner

**Referent für Zivil- und Katastrophenschutz
des Landes Tirol**

Werte PartnerInnen im Zivil- und Katastrophenschutz!

Unser Land ist in erheblichem Maß auf die Funktionsfähigkeit der Stromversorgung und der Informations- und Kommunikationstechnologie angewiesen.

Welche Auswirkungen großflächige Stromausfälle auf eine von Technologie bestimmte Gesellschaft haben können, führten uns weltweit zahlreiche Ereignisse der vergangenen Jahre deutlich vor Augen. Alltäglich verwendete Systeme, die wir als selbstverständlich hinnehmen und die in einer modernen Welt des 21. Jahrhunderts nicht mehr wegzudenken sind, funktionieren ohne Strom schlicht nicht mehr. Lernen wir rechtzeitig daraus!

Gerade auch für solche Situationen hat der Zivil- und Katastrophenschutz vorzusorgen. Zur Hilfeleistung gegenüber Betroffenen müssen Einsätze organisationsübergreifend geführt werden können, so dass die schnellstmögliche Hilfe gewährleistet ist.

Dieses Handbuch bietet zunächst einen umfangreichen und detaillierten Überblick über die bestehenden Technologien. Zudem ermöglicht es dem Benutzer an Hand eines durchgehenden „roten Fadens“, die eigenen Systeme auf Ausfallsicherheit zu überprüfen, mittels Lösungsvorschlägen sowie Tipps und Tricks eine erhöhte Ausfallsicherheit zu erzielen und einen konkreten Einsatzplan zu erarbeiten.

Sie sind eingeladen, im Rahmen der Krisenvorsorge die aus diesem Handbuch resultierenden Maßnahmen in Ihrem Bereich zu prüfen und umzusetzen.

Ich danke allen PartnerInnen im Zivil- und Katastrophenschutz für ihre wertvolle Arbeit und ihren Einsatz um die Sicherheit der Menschen in unserem Bundesland. Möge dieses Handbuch dazu beitragen, bei großflächigen Stromausfällen stets bestmöglich reagieren bzw. agieren zu können.

Innsbruck, September 2008

Anton Steixner
Landeshauptmann-Stellvertreter

Zweck des Handbuches	1
Benutzerhinweise	2
Kap 1 Grundlagen	
1.1 Grundlagen Strom	
1.1.1 Einführung Stromversorgung	5
1.1.2 Ausfallszenario	6
1.1.3 Auswirkungen für Verbraucher	8
1.1.4 Stromversorgung in Tirol	
1.1.4.1 Gesetzliche Grundlagen	11
1.1.4.2 Das Europäische Verbundnetz	12
1.1.4.3 Regelblöcke / Regelzonen	13
1.1.4.4 Übertragungsnetze in Tirol	14
1.1.4.5 Stromproduktion und –verbrauch in Tirol	17
1.1.4.6 Netzwiederaufbau	19
1.1.4.7 ÖBB-Bahnstromleitungsnetz	21
1.1.5 Einführung Notstromversorgung	
1.1.5.1 Netzstrom	23
1.1.5.2 Notstrom	23
1.1.5.3 Unterbrechungsfreie Stromversorgung	24
1.1.5.4 Netzersatzanlagen	26
1.2 Grundlagen IKT	
1.2.1 Einführung IKT	27
1.2.2 Ausfallszenario	29
1.2.3 Auswirkungen für Verbraucher	31
1.2.4 IKT in Tirol	
1.2.4.1 Gesetzliche Grundlagen	33
1.2.4.2 Architektur IKT-Netz	36
1.2.4.3 Telekom Austria – internationale Anbindung	37
1.2.4.4 Telekom Austria – IKT-Netz Österreich	38
1.2.4.5 Telekom Austria – Backbone in Tirol	39
1.2.4.6 Architektur Technologieplattform für Telefon- und Sprachübertragung KT-Netz in Tirol	40
1.2.4.7 Architektur Technologieplattform für Datenübertragung IT(IP)-Netz in Tirol	41
1.2.4.8 Anwendung der Technologieplattformen auf der physikalischen Infrastruktur	42
1.2.4.9 Mobilkom Austria – GSM Abdeckung in Tirol	43
1.2.4.10 Mobiltelefonie in Tirol	44
1.2.4.11 Digitalfunk BOS Austria – Tirol	46
1.2.4.12 Digitalfunk BOS Austria – Netzabdeckung Tirol	50
1.2.4.13 Warn- und Alarmierungssystem Tirol WAS –Tirol	51

1.3	Grundlagen Führungsorganisation	
1.3.1	Standardführungsorganisation im Katastrophenfall	53
1.3.1.1	Führungsorganisation	54
1.3.1.2	Führungsverfahren	55
1.3.1.3	Führungsmittel	57
1.3.2	Katastrophen-Führungsorganisation in Tirol	
1.3.2.1	Führung und Kommunikation der Partner im Zivil- und Katastrophenschutz	58
1.3.2.2	Führungsstab	59
1.3.2.3	Aufgaben Leiter Stabsarbeit und Sachgebiete S1 – S6	60

Kap 2 Checklisten zur Einsatzvorbereitung

2.1	Stromversorgung	61
2.1.1	Gebäude/Strukturen	62
2.1.2	Kommunikation	63
2.1.3	Datenverarbeitung	64
2.1.4	Notstromversorgung	65
2.2	IKT-Versorgung	66
2.2.1	Kommunikationstechnologie	67
2.2.2	Informationstechnologie – physikalische Leitungen	68
2.2.3	Informationstechnologie – Geräte/Systeme	69
2.3	Führungsorganisation	70
2.3.1	Führungsorganisation – Ermittlung der Notwendigkeit	70
2.3.2	Führungsorganisation – Zuweisung der Sachgebiete	71
2.3.3	Führungsorganisation – Verankerung	72
2.3.4	Führungsmittel	73

Kap 3 Lösungsvorschläge

3.1	Stromversorgung	
3.1.1	Netzersatzanlage (NEA) – fest eingebaut	74
3.1.2	Netzersatzanlage (NEA) – mobil	75
3.1.3	Unterbrechungsfreie Stromversorgung (USV)	76
3.1.4	Erhebung Stromverbraucher	77
3.2	IKT	
3.2.1	Grundschutzmaßnahmen IKT	78
3.2.2	Ermittlung der Redundanzen bei Ausfall der Kommunikationstechnologie	79
3.2.3	Redundanzen bei Ausfall IT – physikalische Leitungen	80
3.2.4	Redundanz bzw. Ersatz IT-Geräte/-Systeme	81
3.2.5	Notmaßnahmen IKT – Ausfall Anbieter	82
3.2.6	Notmaßnahmen IKT – Komplettausfall	83
3.3	Führungsorganisation	
3.3.1	Aufbau einer Führungsorganisation	85
3.3.2	Praktische Vorgangsweise	86
3.4	Tipps und Tricks bei Strom- und IKT-Ausfall	
3.4.1	Strom	87
3.4.1	IKT	88

Kap 4 Ausarbeitung des Einsatzplanes

4.1 Inhalt des Einsatzplanes	
4.1.1 Führungsorganisation	91
4.1.2 Alarmorganisation	91
4.1.3 Einsatzszenarien	92
4.1.4 Listen und Verzeichnisse	92
4.2 Vorgangsweise	93

Kap 5 Anhang

5.1 Historische Ausfallereignisse	
5.1.1 Detaillierte Beschreibung	98
5.2 Informationsformulare Landeswarnzentrale	104
5.2.1 Erhebung Führungsorganisation	105
5.2.2 Erhebung Kommunikationsmittel - KT	106
5.3 Ansprechpartner im Zivil- und Katastrophenschutz	107
5.4 Projekt Handbuch Blackout / Impressum	108
5.5 Glossar	110

Zweck des Handbuches

Zweck des vorliegenden Handbuches ist es, allen Tiroler Partnern im Zivil- und Katastrophenschutz Vorbereitungen zur Führung von Einsätzen ohne Netzstrom, Computer und Telefon zu ermöglichen.

Mit Hilfe dieses Handbuches können Vorkehrungen zur Vermeidung von Führungsproblemen, bedingt durch Ausfälle von elektrisch betriebenen Führungsmitteln (Kommunikation, EDV, Anlagen und Ausstattungen), getroffen werden. Vorrangiges Ziel dabei ist es, durch gezielte Präventivmaßnahmen diese Ausfälle betriebsintern zu verhindern oder einzuschränken.

Dazu werden gezielt Informationen über:

1. die Grundlagen der Stromversorgung in Tirol,
2. die Infrastrukturen und die Funktionsweise der Informations- und Kommunikationsnetze (IKT), wie Telefon und Internet,
3. den Aufbau und die Funktionsweise der Führungsorganisation im Zivil- und Katastrophenschutz

im Handbuch zur Verfügung gestellt.

Zusätzlich werden Vorschläge zur Erstellung einer effizienten standardisierten Führungsstruktur bei den Partnern im Zivil- und Katastrophenschutz für den Notfall unterbreitet. Die interne Notfallorganisation unterhalb der Führungsebene der Behörden, Einsatzorganisationen und Unternehmen ist nicht Gegenstand dieses Handbuches.

Unter „Tipps und Tricks“ werden einfache Hilfsmittel bei Strom- und IKT-Ausfällen zur besseren Bewältigung dieser Ausnahmelage genannt.

Mit den zwei Formblättern, die sich im Anhang befinden, sollen der Landeswarnzentrale Tirol Informationen über Führungsorganisation und Kommunikationsmittel der Partner im Zivil- und Katastrophenschutz bereitgestellt werden.

Benutzerhinweise

Mit Hilfe des vorliegenden Handbuches kann jeder Nutzer seine Behörde, Organisation oder Unternehmen auf das Führen von „Einsätzen“ ohne Netzstrom und bei IKT-Ausfall vorbereiten. Wir empfehlen die folgende Vorgangsweise:

Innerhalb der eigenen Organisation sollte eine Person aus der Führungsebene mit der Umsetzung der Empfehlungen des Handbuches beauftragt werden. Es wird vorgeschlagen, die Umsetzung in folgenden fünf Schritten anzugehen:

1. Aneignung von Basiswissen

Im Kapitel Grundlagen wird das notwendige Basiswissen in den Blöcken Strom, IKT und Führungsorganisation vermittelt. Als erster Schritt ist dieser Teil des Handbuches aufmerksam zu lesen.

Strom

Im ersten Block Strom findet der Anwender Informationen über das Zustandekommen eines Blackouts, die möglichen Auswirkungen, die technischen und gesetzlichen Grundlagen der Stromversorgung in Europa, Österreich und Tirol. Erklärt wird der Netzwiederaufbau nach einer Großstörung sowie Netz- und Notstromversorgungsarten.

IKT

Im zweiten Teil Grundlagen IKT sind mögliche Ausfallszenarien im Informations- und Telekommunikationsbereich beschrieben und die zu erwartenden Folgen werden genannt. Nach einem Überblick über die gesetzlichen Grundlagen werden die Netzarchitektur und die Technologieplattformen der IKT-Netze beschrieben.

In kurzen Beschreibungen werden die wichtigsten Informationen über die Mobiltelefonie, das digitale Funknetz der Behörden und Organisationen mit Sicherheitsaufgaben sowie über das Warn- und Alarmsystem dargestellt.

Führungsorganisation

Fachwissen über den Standard in Österreich zum Aufbau einer Führungsorganisation zur koordinierten Führung und zur Sicherstellung der Interoperabilität in Krisen- und Katastrophensituationen wird hier zur Verfügung gestellt.

Einführung

2. Analyse und Einsatzvorbereitung mit Hilfe der Checklisten

Mit Checklisten zur Einsatzvorbereitung zu den Themen Strom, IKT und Führungsorganisation beginnt die praktische Umsetzung des Handbuchs. Durch das Ankreuzen der gestellten Fragen mit ja oder nein und die Auswertung der Antworten werden Informationen über die erforderliche Strom- und IKT-Versorgung gegeben. Ob eine Führungsorganisation gebraucht wird und welche Führungsmittel erforderlich sind, geht nach der Bearbeitung der Checklisten zu diesem Bereich hervor. Über Querverweise („Links“) wird zu Handlungsanweisungen und Lösungsvorschlägen verwiesen.

Diagramm zur Darstellung der Struktur und Nutzung einer Checkliste zur Einsatzvorbereitung:

- Titel:** Checklisten zur Einsatzvorbereitung: Stromversorgung
- Kapitel:** 2.1
- Thema:** Kommunikation
- Nr. Checkliste:** 2.1.2
- Fragestellung:** Welche Kommunikationsmittel sind für die Führung im Einsatzfall erforderlich?
- Antwort Spalte 1:** ja
- Antwort Spalte 2:** nein
- Auswertung:** Bei einem oder mehreren angekreuzten Kästchen in der Spalte: Notstromversorgung erforderlich
- Auswertung:** Notstromversorgung für angekreuzte Kommunikationsmittel nicht erforderlich
- Link zu weiterführenden Dokumenten:** Checkliste 2.1.4

Kommunikationsmittel	ja	nein
Analoges Telefon ¹		
Digitales Telefon – Erstgerät an ISDN-Basisanschluss ²		
Digitales Telefon – weitere Geräte an ISDN-Basisanschluss ³	ja	nein
Digitales Telefon – Geräte an ISDN-Multi- od. Primaryanschluss ⁴	ja	nein
Mobiltelefon mit Netz-Aufladegerät	ja	nein
Mobiltelefon nur mit Pkw-Aufladegerät		ja
Fax	ja	nein
PC – E-Mail	ja	nein
Funk-Fixstation	ja	nein
Mobilfunk mit Netz-Aufladegerät	ja	nein
Mobilfunk nur mit Pkw-Aufladegerät		ja
Satellitentelefon mit Netz-Aufladegerät	ja	nein
Satellitentelefon nur mit Pkw-Aufladegerät		ja

¹ Analoge Telefone (POTS) benötigen keine lokale Stromversorgung
² Ein digitales Telefon an ISDN-Basisanschluss benötigt bei richtiger Installation keine lokale Stromversorgung
³ Weitere digitale Telefongeräte an ISDN-Basisanschluss benötigen die lokale Stromversorgung
⁴ Telefongeräte an Multi- oder Primaryanschluss benötigen immer die lokale Stromversorgung

3. Lösungsvorschläge prüfen und umsetzen

Lösungsvorschläge werden in diesem Kapitel zu den Bereichen Strom- bzw. Notstromversorgung, IKT-Grundschutz, Redundanz-, Ersatz- und Notmaßnahmen bei IKT-Ausfall und zum Aufbau einer Führungsorganisation unterbreitet. Diese sind an die eigene Organisation anzupassen und umzusetzen.

Weiters werden „Tipps und Tricks“ bei Strom- und IKT-Ausfall aufgezeigt.

4. Den Einsatzplan erarbeiten

Die Strukturierung und der erforderliche Inhalt eines Einsatzplanes werden im Kapitel Erarbeiten des Einsatzplanes aufgezeigt. Auf dieser Grundlage kann ein Einsatzplan erstellt oder ein bestehender angepasst werden.

5. Nicht zuletzt: Den Anhang genau durchsehen

Im Anhang sind wichtige Unterlagen und Informationen zu finden:

- Das Glossar
- Eine detaillierte Beschreibung von historischen Ausfallereignissen
- Formblätter zum Ausfüllen und Übermitteln an die Landeswarnzentrale

1.1.1 Einführung Stromversorgung

Zum Einstieg in die komplizierte Materie der Stromversorgung und des Zustandekommens von Blackouts werden die wichtigsten Fakten nachfolgend beschrieben. Vorab werden die Begriffe „Störung in der Stromversorgung“ und „Blackout“ definiert :

Bei einem Stromausfall auf lokaler Ebene, meist im Einflussbereich eines Versorgers oder Netzbetreibers, spricht man von einer „Störung der Stromversorgung“. Ein „Blackout“ hingegen ist der vollständige und großflächige Ausfall der Stromversorgung auf regionaler und überregionaler Ebene. Blackouts werden auch als Großstörung bezeichnet.

Grundlagen der Stromversorgung

Elektrische Energie muss im selben Augenblick erzeugt werden, in dem sie verbraucht wird. Kleinere Schwankungen im Verbrauch (bis zu 2,5 %) werden durch automatische Regler an den laufenden Turbinen durch Erhöhung oder Senkung der Drehzahlen aufgefangen. Diese Primärregelung verteilt die Verbrauchsschwankungen auf die Kraftwerke im gesamten Verbundsystem. Wenn der Strombedarf höher ist als die Produktion, sinkt die Frequenz, gemessen in Hertz (Hz). Mit der Frequenz als Indikator wird die Stromversorgung an den aktuellen Verbrauch angepasst.

Steigt der Bedarf über die Schwankungsbreite der Primärregelung, so muss der zuständige Dispatcher (Koordinator, Zuteiler) des Regelzonenführers im Bereich mit gestiegenem Bedarf innerhalb von Minuten zusätzliche Kraftwerke an das Netz hängen. Dies erfolgt in der Regel mittels Wasserkraft oder mit Gasturbinen betriebenen Kraftwerken. Diese Maßnahmen können von den Diensthabenden in den Netzleitstellen per Mausclick oder mit einem Telefonanruf eingeleitet werden. Im äußersten Notfall müssen Verbraucher durch Abschaltungen von Leitungen vom Netz genommen werden, damit das Gesamtsystem nicht gefährdet wird.

Sinkt der Verbrauch, kommt es zu einem Anstieg der Frequenz. Auch hier besteht Handlungsbedarf: Es gilt Kraftwerke abzuschalten oder Verbraucher, wie Pumpspeicherwerke zuzuschalten. Wird nichts unternommen, werden die Leitungen durch automatische Sicherungen abgeschaltet.

Zu hohe oder zu niedere Frequenzen schädigen die Generatoren und die Geräte der Endverbraucher.

1.1.2 Ausfallszenario

Großflächige Stromausfälle werden meist durch einen Defekt in einem Elektrizitätswerk, die Beschädigung einer elektrischen Leitung, einen elektrischen Kurzschluss oder eine lokale Überlastung des Stromnetzes verursacht. Überregionale Stromnetze werden nach dem n-1 Kriterium (sprich n minus 1) betrieben. Dies bedeutet, dass zu jeder Zeit entweder ein elektrisches Betriebsmittel oder ein Transformator, eine Leitung oder ein Kraftwerk ausfallen darf, ohne dass es zu einer Überlastung eines anderen Betriebsmittels kommen darf oder gar zu einer Unterbrechung der Energieversorgung.

Aus diesem Grund werden in Österreich und im Gebiet der Union for the Coordination of Transmission of Electricity, zu Deutsch: Union für die Koordinierung des Transports von Elektrizität (UCTE), dem Zusammenschluss von 34 europäischen Übertragungsnetzbetreibern (siehe 1.1.4.2, Grafik Mitgliedsstaaten der UCTE), die Stromnetze im Verbund geführt. Trotzdem ist es in der Vergangenheit durch „unglückliches“ Zusammentreffen mehrerer nachteiliger Umstände zu großflächigen Blackouts gekommen.

Auswirkungen eines Ausfalls im gestörten Netz

Zur Aufrechterhaltung einer stabilen Versorgung müssen Stromproduktion und Stromverbrauch immer ausgeglichen sein. Steigt der Strombedarf, müssen sofort Ersatzleistungen herangeschafft werden. Können in einem solchen Fall z.B. auf Grund von Kommunikationsproblemen Spitzenlastkraftwerke nicht ausreichend mobilisiert, oder Ersatzleitungen nur unzureichend geschaltet werden, können größere Ausfälle die Folge sein. Lässt sich für den momentanen Bedarf im eigenen Netz nicht genügend Energie aktivieren, sinken sowohl die Netzspannung als auch (was wichtiger ist) die Netzfrequenz, denn in diesem Fall ist im Netz der Verbrauch höher als die erzeugte Leistung. Unterschreitet die Frequenz einen bestimmten Wert (üblich sind z.B. 47,5 Hertz [Hz]), wird das Kraftwerk durch automatische Schutzeinrichtungen vom Netz getrennt, um Beschädigungen der Turbine zu vermeiden.

Kann das Netz in einem solchen Fall nicht durch Stromeinspeisung von benachbarten Netzabschnitten stabilisiert oder durch gezielten Lastabwurf - d.h. das Abschalten oder Abtrennen von großen Verbrauchern - der Strombedarf verringert werden, kommt es zu

automatischen regionalen Stromabschaltungen, um wenigstens im Rest des Netzes eine Versorgung aufrechtzuerhalten. Reagiert diese Netzregelung nicht oder zu träge, so dass Nachbarnetze das eigene Netz nicht stützen können, kommt es zu einem Gesamtausfall des Netzes.

In diesem Fall kann es zu einem stärkeren Absinken der Netzfrequenz kommen. Dies würde an den Verbindungsstellen zu funktionierenden Netzen zu sehr hohen Ausgleichströmen führen, so dass hier die Sicherungen ausgelöst würden. Fällt die Stützung des Netzes durch Nachbarnetze aus, sinkt die Netzfrequenz weiter. Ist auch kein gezielter Lastabwurf möglich (wird normalerweise durch automatische Regelung ohne menschliches Zutun durchgeführt), sinkt die Netzfrequenz unter eine kritische Grenze, und das Netz schaltet sich automatisch ab.

Die Netzregelung, die für den Ausgleich von Verbrauch und Erzeugung in den ersten kritischen Augenblicken verantwortlich ist, funktioniert ohne Eingriff eines Menschen und reagiert sehr schnell. Damit es zum Blackout eines gesamten Netzes kommt, müssen in der Regel mehrere Ereignisse zusammentreffen.

Auswirkungen in Nachbarnetzen

Das Zusammenbrechen eines Netzes hätte auch Auswirkungen auf die umgebenden Netze. Es fehlt plötzlich ein großer Stromverbraucher, so dass die Netzfrequenz ohne weitere Maßnahmen zu stark steigen würde. In diesem Fall wird versucht, die Stromproduktion z.B. durch ein schnelles Herunterfahren von Spitzenlast-Kraftwerken zu drosseln. Zusätzlich werden Maßnahmen ergriffen, um den Stromverbrauch zu erhöhen, wie z.B. das Starten der Pumpen in Pumpspeicherwerken, Einschalten von Stromverbrauchern per Rundsteuertechnik (Leistungserhöhung bei industriellen Verbrauchern, Aufheizen von Nachtspeicherheizungen), verstärkte Abgabe in Nachbarnetze.

Gelingt es nicht, den Wegfall des gestörten Netzes zu kompensieren, steigt im Nachbarnetz die Netzfrequenz zu stark an. Dies führt dazu, dass sich das betroffene Netz zuerst wegen zu großer Unterschiede in der Netzfrequenz von den Nachbarnetzen trennt und sich dann bei zu hoher Netzfrequenz selbst abschaltet.

Bezieht ein Nachbarnetz erhebliche Mengen Strom aus dem gestörten Netz, muss auch hier die Netzregelung auf den Wegfall der Stromeinspeisung reagieren.

1.1.3 Auswirkungen für Verbraucher

Blackouts, d.h. Großstörungen in der Stromversorgung, haben ein hohes Bedrohungspotenzial. Länger andauernde Ausfälle haben schwerste Auswirkungen auf das tägliche Leben. Ohne Strom bricht das gewohnte tägliche System, in dem wir leben, zusammen.

Bedroht sind dabei:

1. Das Leben und die Unversehrtheit der Menschen
2. Die Aufrechterhaltung der öffentlichen Sicherheit
3. Die Ver- und Entsorgung von Gütern des täglichen Bedarfes
4. Die Telekommunikation und das Transportwesen
5. Die Aufrechterhaltung der Produktion in Landwirtschaft, Industrie und Gewerbe

Die Folgen für:

1. Das Leben und die Unversehrtheit der Menschen

Verletzte, Erkrankte und Tote durch:

- Ausfall von Ampel- und Signalanlagen
- Stürze in der Dunkelheit
- Ausfall von lebenserhaltenden Systemen und Sicherheitseinrichtungen
- Ausfälle von Beatmungsgeräten
- Verdorbene Lebensmittel durch Ausfall von Kühleinrichtungen
- Probleme in Krankenhäusern:
Die Notstromversorgung deckt nur die wichtigsten Verbraucher,
keine Redundanz bei Ausfall der Notstromversorgung z.B. durch
Treibstoffmangel
- Ausfall von Trinkwasseraufbereitungsanlagen

2. Die Aufrechterhaltung der öffentlichen Sicherheit

- Verbrechen in der Dunkelheit
- Notrufnummern von Rettung, Polizei und Feuerwehr sind wegen Überlastung nicht erreichbar
- Ausfall von Alarm- und Sicherheitseinrichtungen
- Unkontrollierbare Reaktionen der Anwesenden aufgrund von Ausfall der Beleuchtung in Räumen und Bereichen mit hoher Menschendichte (z.B. Veranstaltungsräumen, Kaufhäusern, usw.)
- Ausfall von Funkeinrichtungen bei Behörden
- Ausfall von Notstromaggregaten durch Treibstoffmangel bei Behörden und Einsatzorganisationen (BOS)
- Hohe Sicherheitsrisiken durch Notabschaltungen in Chemiebetrieben

3. Die Ver- und Entsorgung von Gütern des täglichen Bedarfs

- Durch Ausfall von EDV-Systemen vielfach Probleme bei der Versorgung mit allen Gütern des täglichen Bedarfs
- Ausfall von Warenwirtschaftssystemen und Registrierkassen, kein Verkauf und keine Auslieferung möglich
- Ausfall von vollautomatischen Hochregallagern, keine Auslieferung
- Ausfall von Transportdiensten durch Treibstoffmangel
- Ausfall von Bankdiensten und Bankomaten, kein Bargeld verfügbar
- Ausfall der Trinkwasserversorgung
- Trinkwasserverschmutzung durch Ausfall von Desinfektionsanlagen
- Verderben von Frischprodukten durch Ausfall der Kühlanlagen
- Ausfall der elektrisch betriebenen Heizanlagen (auch Gas-, Öl- und Hackschnitzelheizungen)
- Ausfall von Küchenanlagen
- Ausfall der elektrisch betriebenen Koch- und Küchengeräte in Privathaushalten
- Probleme bei der Abwasserentsorgung durch Ausfall von Pumpen und Steuerungsanlagen

4. Die Telekommunikation und das Transportwesen

- Zusammenbruch Eisenbahn- und Straßenbahn, Seilbahnen, Lifte, usw.
- Tausende festsitzende Reisende
- Probleme auf Straßen und in Tunnels durch Ausfall der Sicherheitseinrichtungen
- Ausfall der Treibstoffversorgung an Tankstellen infolge Ausfall der Treibstoffpumpen
- Kommunikationsprobleme bei den Telefondiensten durch Ausfälle im Mobil- und Festnetz
- Ausfall von Internet, E-Mail und der Datenübertragung

5. Die Aufrechterhaltung der Produktion in Landwirtschaft, Industrie und Gewerbe

- Ausfall der Melk-, Fütterungs- und Entmistungsanlagen in Tierzuchtbetrieben
- Ausfall von Heizanlagen in Gartenbaubetrieben mit Glashäusern
- Produktionsunterbrechung in Betrieben
- Lebensmittelproduktion und Frischproduktverarbeitung z.B. Milchverarbeitung durch Ausfall der Produktions- und Kühlanlagen
- Verdorbene Lebensmittel bei Produzenten und Versorgern aufgrund von Ausfall der Kühlanlagen
- Produktionsunterbrechungen in Betrieben ohne Notstromversorgung und bei Ausfall von Transportdiensten durch Mangel an Rohstoffen bzw. Halbfertigprodukten
- Hohe Sicherheitsrisiken durch Notabschaltungen in Chemiebetrieben

Im Anhang sind historische Stromausfälle mit Folgen und Auswirkungen beschrieben. Dies verdeutlicht weiter die massiven Probleme, die bei Stromausfällen auftreten.

Sicher ist eines: Längerfristige Stromausfälle können den kompletten Zusammenbruch unserer gewohnten Lebensumstände bewirken.

1.1.4 Stromversorgung in Tirol

1.1.4.1 Gesetzliche Grundlagen

In den Richtlinien 90/547/EWG, 90/377/EWG und 96/92/EG (<http://www.iee.tugraz.at/ewirtschaft/download/EURichtlinie.pdf>) über den Elektrizitätsbinnenmarkt sind die Rahmenbedingungen für die Liberalisierung des Strommarktes und damit der Stromversorgung in Europa festgelegt worden. Diese sind am 19.2.1997 in Kraft getreten. Die praktischen Auswirkungen dieser Bestimmungen sind in erster Linie die Trennung der Bereiche der Elektrizitätswirtschaft in „Erzeugung“, also die Produktion von Strom in Kraftwerken, in „Übertragung“, den Transport von Elektrizität über das Netz und in den „Vertrieb“, den Verkauf an den Kunden. Dies ist notwendig, um den Elektrizitätsmarkt für den Verbraucher vollständig zu öffnen, den freien Stromhandel zu ermöglichen und den Netzzugang für Produzenten, Händler und Kunden zu gewährleisten. EU-Richtlinien wirken indirekt und müssen erst von den Mitgliedsstaaten durch nationale Gesetze umgesetzt werden. Dies ist in Österreich mit dem Elektrizitätswirtschafts- und Organisationsgesetz (ELWOG), BGBl. I Nr. 143/1998, geschehen.

Durch das ELWOG wurde den einzelnen Bundesländern die Kompetenz übertragen, entsprechende Ausführungsgesetze zu erlassen. In diesen Gesetzen sind detaillierte Bestimmungen über die Genehmigung von Anlagen, Einrichtung eines Regelzonenführers, Bildung von Bilanzgruppen udgl. enthalten.

In Tirol ist dies das Tiroler Elektrizitätsgesetz 2003, TEG LGBl.Nr. 88/2003, i.d.F.LGBl.Nr. 83/2005 und LGBl.Nr. 17/2007.

1.1.4.2 Das Europäische Verbundnetz

Das Tiroler Übertragungsnetz ist mit dem nationalen Versorgungsnetz Österreichs in das große europäische Verbundnetz der Union for the Coordination of Transmission of Electricity (UCTE), welches aus dem Zusammenschluss der Netze von insgesamt 23 europäischen Ländern besteht und rund 450 Millionen Menschen mit elektrischer Energie versorgt, im synchronen Parallelbetrieb zusammengeschaltet.

Dieses europäische Netz ermöglicht den Austausch von Energie und dient auf der einen Seite der Erhöhung der Sicherheit in der Stromversorgung. Probleme wie Engpässe in nationalen Netzen können durch gegenseitige Interventionen gelöst werden. Andererseits sind damit auch Risiken verbunden. Massive Störungen an einer Stelle haben Auswirkungen auf das gesamte Netz. Die UCTE erstellt Regeln und Richtlinien für den gemeinsamen Netzbetrieb. Die Führung eines Verbundnetzes ist nur möglich, wenn alle daran beteiligten Netzbetreiber gemeinsam erarbeitete, globale Regeln befolgen, wie z. B. die Regelung der gemeinsamen Frequenzhaltung oder das Prinzip, dass bei Ausfall eines einzelnen Netzelementes bei den verbleibenden Netzelementen keine unzulässige Belastung auftreten darf.

Dazu haben sich die Mitglieder des UCTE-Netzverbunds auf gemeinsame Normen und Regeln geeinigt, die im sogenannten „Operation Handbook“ festgeschrieben sind und über einen multilateralen Vertrag zwischen den beteiligten Netzbetreibern (MLA = Multilateral Agreement) verpflichtend abgesichert wurden. Verstöße gegen diese Regeln ziehen gravierende Strafen nach sich.

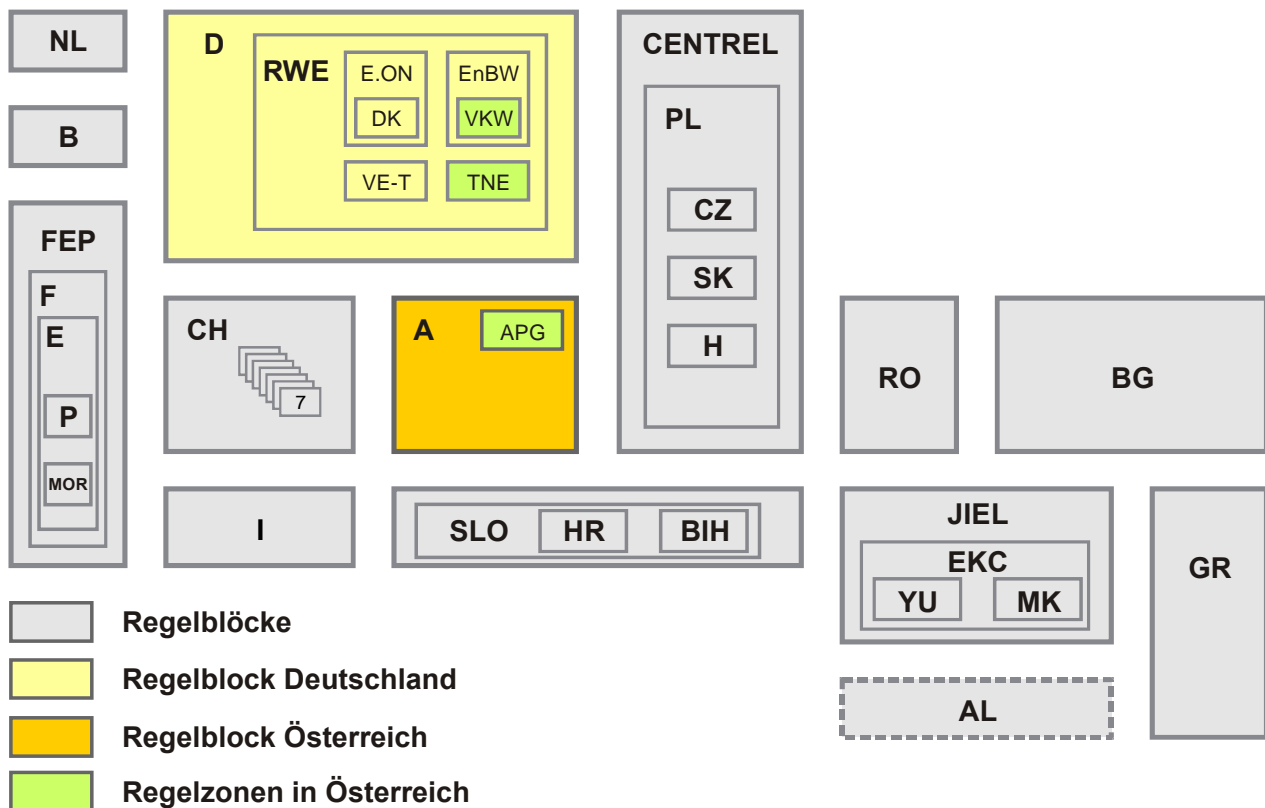


Grafik Mitgliedsstaaten der UCTE

(Quelle: UCTE, Stand 2007)

1.1.4.3 Regelblöcke / Regelzonen

Das europäische Verbundnetz der UCTE ist in Regelblöcke und diese wiederum zum Teil in Regelzonen gegliedert. Ost-Österreich bildet einen Regelblock. Regelblockführer und Übertragungsnetzbetreiber für Ost-Österreich ist die Austrian Power Grid (Verbund APG). Die Regelzonen Tirol und Vorarlberg sind aufgrund der energiewirtschaftlichen Ausrichtung nach Süddeutschland dem deutschen Regelblock zugeordnet. Regelblockführer für den Block Deutschland ist die RWE Transportnetz Strom GmbH in Brauweiler.



TNE: TIWAG-Netz AG

VKW: VKW-Netz AG

APG: Austrian Power Grid (Verbund)

Grafik Regelblöcke / Regelzonen in der UCTE

(Quelle: UCTE, TIWAG-Netz AG Stand 2008)

- Regelblock Österreich: Netzbereich Ost – Regelzonenführer Austrian Power Grid
- Regelblock Deutschland: Regelzone Tirol – Regelzonenführer TIWAG-Netz AG
- Regelblock Deutschland: Regelzone Vorarlberg – Regelzonenführer VKW-Netz AG



Grafik Regelzonen in Österreich

(Quelle: TIWAG-Netz AG, Verbund, Stand 2008)

Die TIWAG-Netz AG ist als Regelzonenführer verantwortlich für die jederzeitige Leistungs- und Frequenzregelung , sowie für den möglichst raschen Wiederaufbau der Stromversorgung in der Regelzone nach einem großflächigen Stromausfall. Die Zentrale Netzleitstelle der TIWAG-Netz AG befindet sich in Thaur. In Verbindung mit den Tiroler Großerzeugungsanlagen gewährleistet die TIWAG-Netz AG die Versorgungssicherheit für die Tiroler Bevölkerung und Wirtschaft.

1.1.4.4 Übertragungsnetze in Tirol

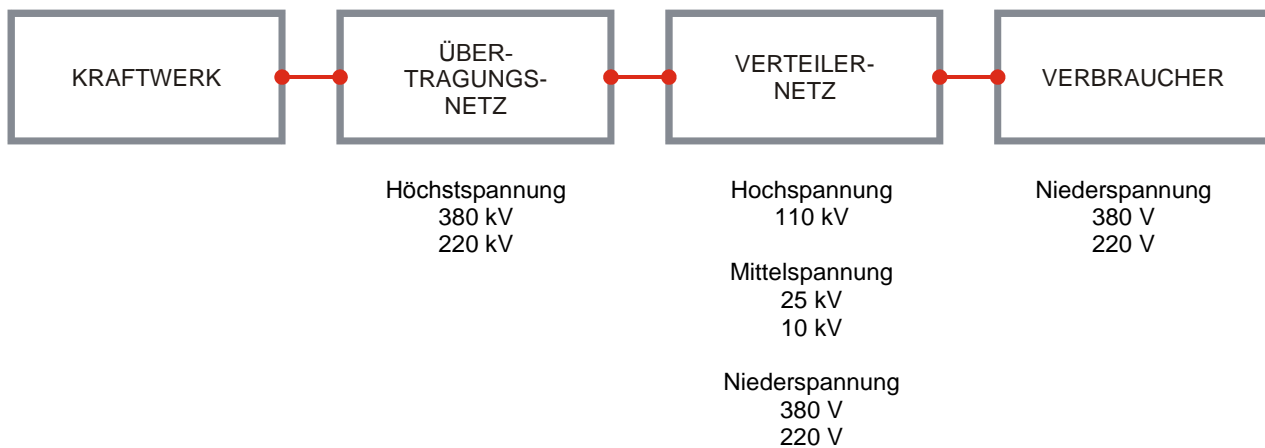
Das Übertragungsnetz stellt das Rückgrat der Stromversorgung dar.

Das Übertragungsnetz ist ein Höchstspannungsverbundnetz mit einer Spannungshöhe von 380 kV und 220 kV. Es dient dem überregionalen Transport von elektrischer Energie.

In Tirol werden Übertragungsnetze von der TIWAG-Netz AG, der VERBUND-Austrian Power Grid AG und über den Arlberg von der Vorarlberger Illwerke AG betrieben.

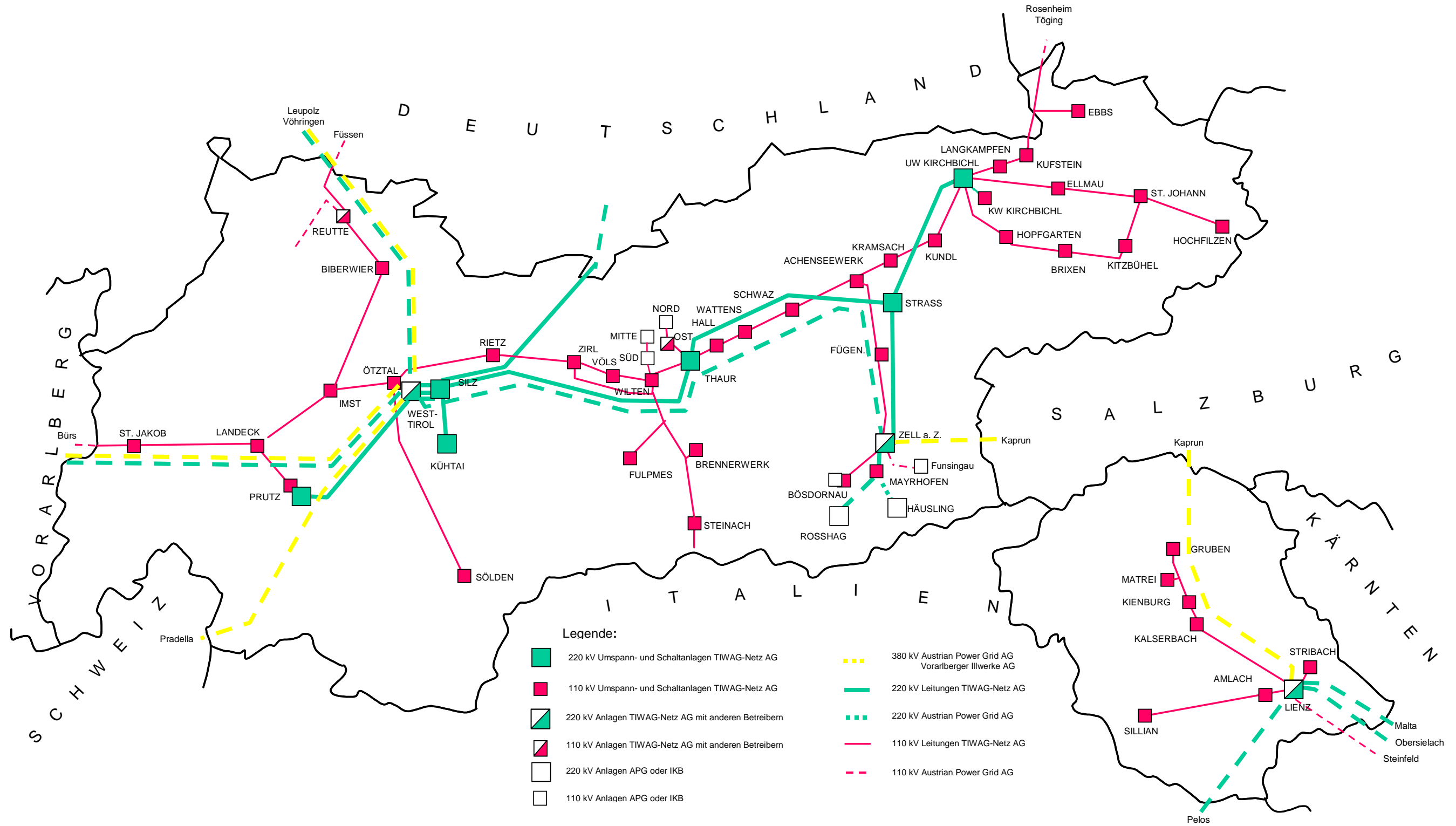
Über Transformatoren wird der Strom aus den Übertragungsnetzen (Höchstspannungsnetz) in die Verteilernetze eingespeist (Hochspannungsnetz 110 kV und Mittelspannungsnetz).

Die Mittelspannungsnetze werden mit einer Spannung von 25 kV – 10 kV betrieben. Zum Verbraucher gelangt die elektrische Energie über die Niederspannungsnetze. Dabei wird der Strom aus den Mittelspannungsnetzen auf eine Spannung von 380 V bzw. 220 V reduziert.



Grafik Stromverteilung in Tirol

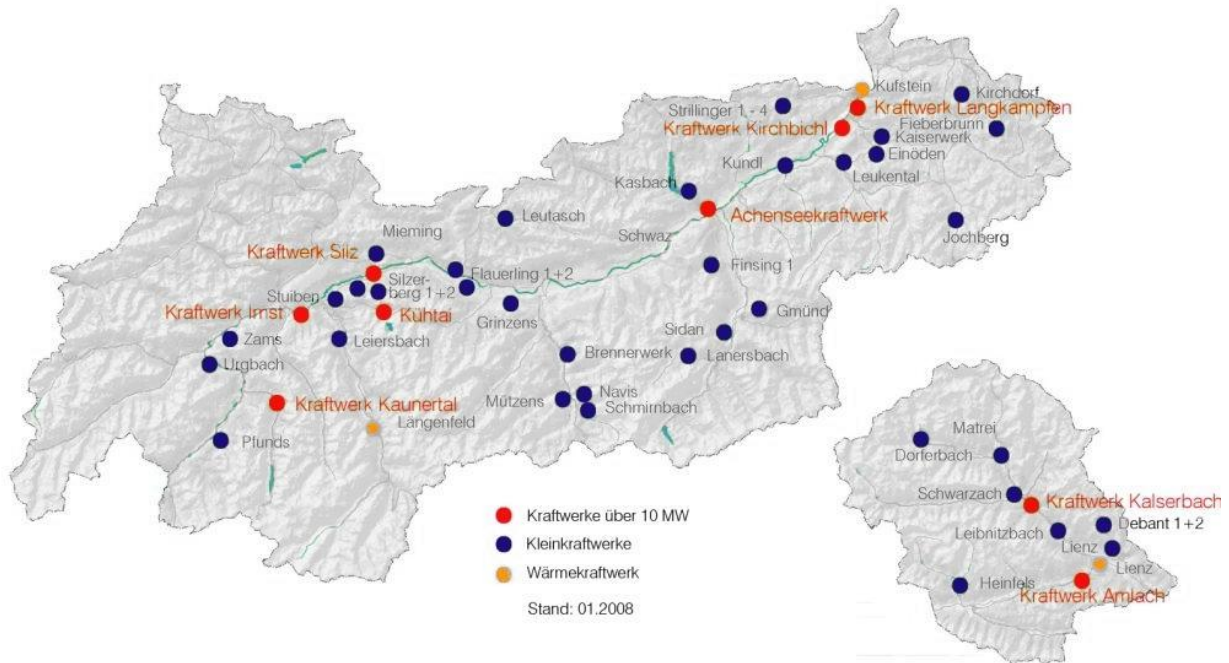
380kV/220kV/110kV Netz in Tirol



Grafik Höchst- und Hochspannungsnetze in Tirol

(Quelle: TIWAG-Netz AG, Stand 2008)

1.1.4.5 Stromproduktion und -verbrauch in Tirol



Grafik Kraftwerksanlagen in Tirol

(Quelle: TIWAG-Netz AG, Stand 2008)

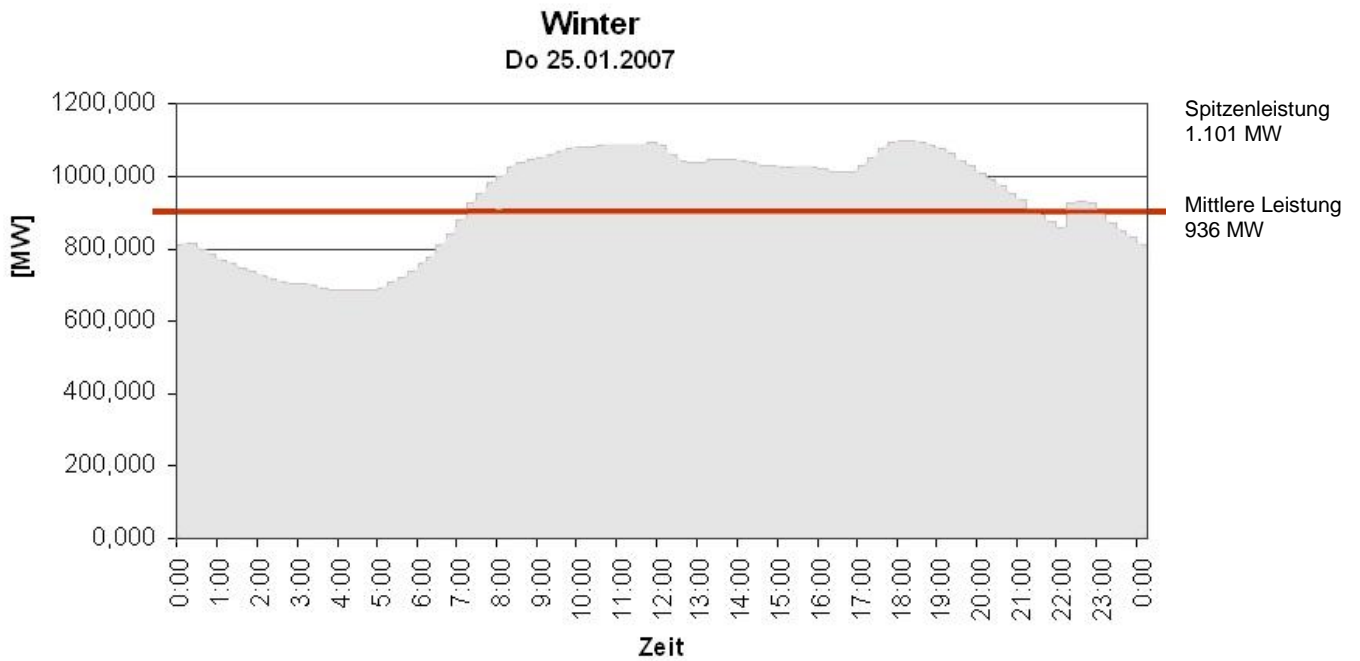
In Tirol installierte Kraftwerksleistung:

140 Laufkraftwerke mit einer EPL *	540 MW
19 Speicherkraftwerke mit einer EPL	2.358 MW
17 Wärmekraftwerke mit einer EPL	42 MW

Stromverbrauch in Tirol:

Spitzenleistung	1.101 MW
Mittlere Leistung am Spitzentag	936 MW

***EPL:** Die Engpaßleistung ist die maximale Dauerleistung, die ein Kraftwerk unter Normalbedingungen abgeben kann.



Grafik Landesverbrauch Spitzentag Do 25.01.2007 in MW

(Quelle: TIWAG-Netz AG)



Grafik Netzlast Innsbruck gewöhnlicher Wintertag in MW

(Quelle: TIWAG-Netz AG)

1.1.4.6 Netzwiederaufbau

Der Regelzonenführer für Tirol, die TIWAG-Netz AG, ist verantwortlich für die Wiederherstellung der Stromversorgung nach einer Großstörung (Blackout).

Zu diesem Zweck verfügt die TIWAG-Netz AG über ein Netzwiederaufbaukonzept und hat dafür ein internes Krisenmanagement aufgebaut.

Nach einem Blackout sieht das Netzwiederaufbaukonzept den Aufbau eines autarken Inselbetriebes in Tirol mit Tiroler Großkraftwerken vor. Alle Verbindungen des Tiroler Übertragungsnetzes werden dabei zu anderen Netzen unterbrochen.

Tirol ist in der glücklichen Lage vorübergehend den eigenen Strombedarf durch die Tiroler Wasserkraftwerke decken zu können.

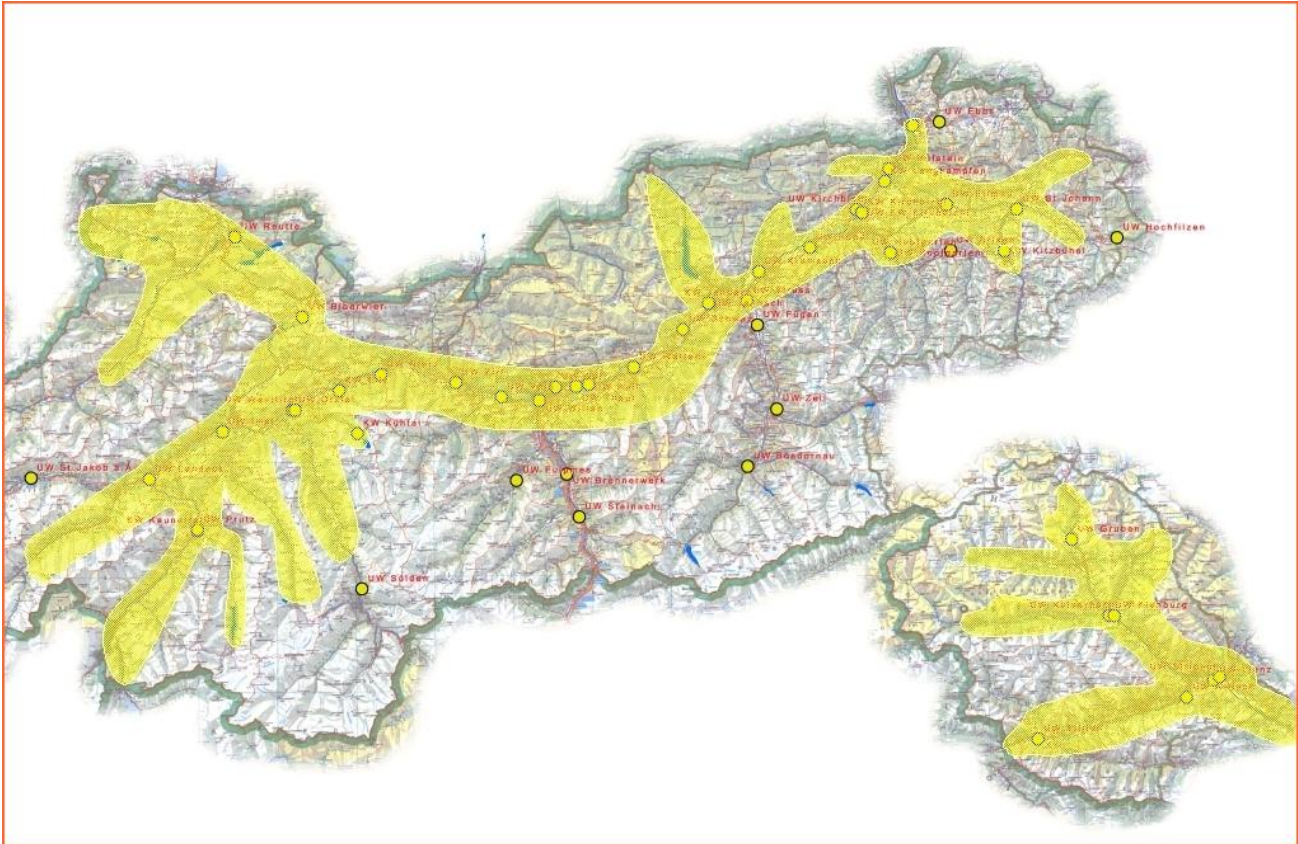
Das Netzaufbaukonzept sieht vor, sobald eine „gesunde“ UCTE-Spannung an den Verbindungsstellen des Tiroler Netzes ansteht, das Tiroler „Inselnetz“ wieder mit dem UCTE-Netz zusammenzuschalten.

Bei schlechtesten Bedingungen (leere Stauseen im Frühjahr) wird mit einer Mindestversorgungsdauer des Tiroler Inselnetzes mit den eigenen Kraftwerken von ca. einer Woche gerechnet.

Das Netzwiederaufbaukonzept sieht in Abweichung zum Normbetrieb anstelle der üblichen Frequenz von 50Hz eine höhere Schwankungsbreite der Frequenz von 50,2 – 51,5 Hz im Inselbetrieb vor. Im Extremfall kann die Frequenz kurzzeitig bis 49,2 Hz nach unten und 52,5 Hz nach oben ausschlagen. Geräte und Anlagen, die für das Krisenmanagement gebraucht werden, sollten auf ihre Funktionalität unter diesen Bedingungen überprüft werden.

Der Zentralraum kann nach Beginn des Netzwiederaufbaues nach ca. 180 Min. wieder mit Strom versorgt werden.

Die Peripherie wird anschließend schrittweise zugeschaltet.



Grafik Netzwiederaufbau im Zentralraum Tirol

(Quelle: TIWAG-Netz AG, Stand 2008)

1.1.4.7 ÖBB – Bahnstromleitungsnetz 110/55/15kV 16,7 Hz Einphasenwechselstrom**Traktionsstrom**

Die Österreichischen Bundesbahnen betreiben ein eigenes Bahnstromnetz, bestehend aus einem Übertragungsleitungsnetz (55/110kV, 16,7 Hz Einphasenwechselstrom wie in der Abbildung unten gezeigt), das die Traktionsstromanlagen (Oberleitungsanlagen betrieben mit 15 kV, 16,7 Hz Einphasenwechselstrom) über Unterwerke (Umspannwerke) versorgt.

Unter Bahnstrom wird der „Traktionsstrom“ verstanden, welcher für den Antrieb der Züge gebraucht wird. Das Bahnstromnetz ist zum Teil unabhängig vom öffentlichen Stromnetz. Das Bahnstromnetz wird sowohl von unabhängigen bahneigenen Kraftwerksanlagen als auch vom öffentlichen Netz über Umformerstationen gespeist.

Im Falle eines Ausfalles im öffentlichen Netz kann das Bahnstromnetz regional weiterbetrieben werden.

Die ÖBB verfügt über ein Konzept, mit welchem bei Ausfall des Traktionsstromes die Züge mit ÖBB-eigenen Mitteln (Dieselloks) in den nächsten Bahnhof gebracht werden können.

Stromversorgung von Sicherungsanlagen

Bei der Stromversorgung von Sicherungsanlagen wird zwischen Betriebsführungszentrale (BFZ) und Unterstation (Sicherungsanlage ferngesteuerter Bahnhof) unterschieden. Die Unterstation wird mittels einer USV (Unterbrechungsfreien Stromversorgung) von zwei unabhängigen Netzen versorgt. Zum einem durch das 50 Hz Ortsnetz (400 V) und zum anderen durch das 16,7 Hz Bahnstromnetz (15 KV über Trafo aus Fahrleitung auf 400 V). Die beiden Netze werden über eine USV-Anlage (durch Zwischenschalten von Batterien) unterbrechungsfrei umgeschaltet. Ebenso ist bei Ausfall beider Versorgungsnetze (50 Hz und 16,7 Hz), mittels der dazwischen geschalteten Batterien, ein 20-minütiger Betrieb möglich. Um die Verfügbarkeit einer BFZ zu erhöhen, werden zwei USV-Anlagen, wobei jede alleine die volle Leistung der BFZ abdeckt, aufgebaut um einem theoretischen USV-Anlagenausfall entgegenzuwirken. Daraus ergibt sich zusätzlich eine Verdoppelung der Batterieleistung (Weiterbetrieb von 40 Minuten bei Ausfall beider Netze). Es ist bei der Stromversorgung der BFZ auch eine zusätzliche Versorgung (als „drittes Versorgungsnetz“) mittels Dieselaggregat möglich (sofern ein Anschluss für ein fahrbares Aggregat vorhanden ist)!

Stromversorgung weiterer Anlagen

Die Beleuchtung der Bahnhöfe und Haltestellen, sowie die Anzeigen für Fahrgäste werden über das öffentliche Netz versorgt. Im Falle eines Blackouts fallen diese Anlagen aus.



Legende:

	500 mm ²				Kraftwerk				Bahnfremdes Kraftwerk
	300 mm ²				Umformerwerk				Bahnfremdes Unterwerk
	260 mm ²				Umrichterwerk				Kompensationsanlage
	240 mm ²				Pumpwerk				Übertragungsleitung 110 kV
	210 mm ²				Unterwerk				Übertragungsleitung 55 kV
	189 mm ²				Fahrbares Unterwerk				Speiseleitung 15 kV
	185 mm ²				Netzkupplung				Elektr. Strecken
	150 mm ²				Kuppelstelle				
180, 1161A	Leitungs Nr.				Schaltposten				
1 2 3 4 1+2	Schleifen Nr.				Schaltstelle				

Grafik Bahnstromleitungsnetz

(Quelle: ÖBB, Stand 2007)

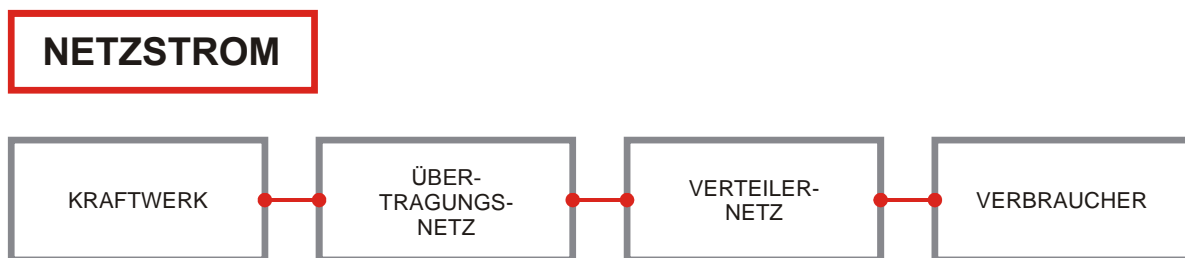
1.1.5 Einführung Notstromversorgung

Eine Notstromversorgung wird dann benötigt, wenn aus irgendwelchen Gründen die Stromversorgung aus dem Netz ausfällt und Gebäude, Anlagen und Einrichtungen weiterbetrieben werden müssen.

1.1.5.1 Netzstrom

Netzstrom ist der Strom, welcher aus dem Netz eines Anbieters zur Verfügung gestellt wird. Über ein Stromnetz werden viele Verbraucher versorgt.

Der Kunde hat dabei keinen Einfluss auf die Versorgungssicherheit.

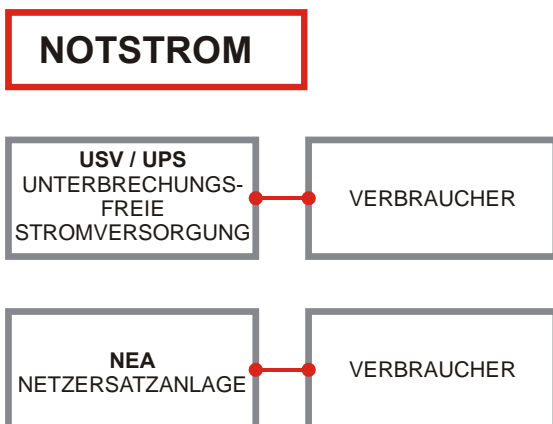


Grafik Netzstromversorgung

1.1.5.2 Notstrom

Notstrom wird zum Ersatz der Netzstromversorgung gebraucht. Notstrom kann dabei aus zwei Quellen zur Verfügung gestellt werden:

1. Aus Batterien (Unterbrechungsfreie Stromversorgung, siehe Erklärung Kap. 1.1.5.3)
2. Von Netzersatzanlagen (NEA – Notstromaggregaten, siehe Erklärung Kap. 1.1.5.4)



Grafik Notstromversorgung

1.1.5.3 Unterbrechungsfreie Stromversorgung – USV

Die Notstromversorgung aus Batterien wird als USV (unterbrechungsfreie Stromversorgung) oder UPS (Uninterruptible Power Supply) bezeichnet. Sie stellt bei Ausfall der Stromversorgung aus dem Netz die unterbrechungsfreie Versorgung der Stromverbraucher sicher.

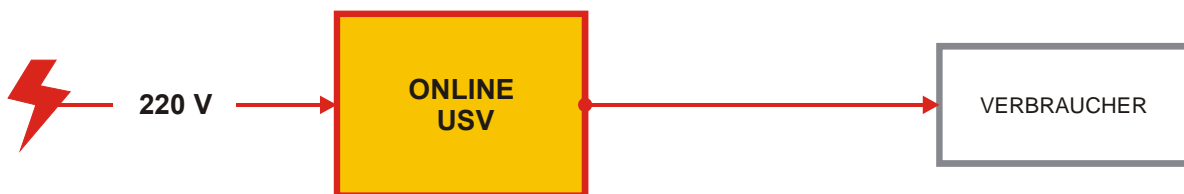
Die unterbrechungsfreie Versorgung ist vor allem bei Sicherheitssystemen, Servern, IT-Anlagen und anderen Einrichtungen erforderlich, bei denen bereits bei kürzesten Versorgungsunterbrechungen große Schäden, oder nicht schnell wieder herstellbare Funktionsausfälle entstehen. USV-Anlagen sind in der Leistung limitiert.

Oft werden diese eingesetzt, um das sichere Herunterfahren von IT-Anlagen und Servern zu ermöglichen.

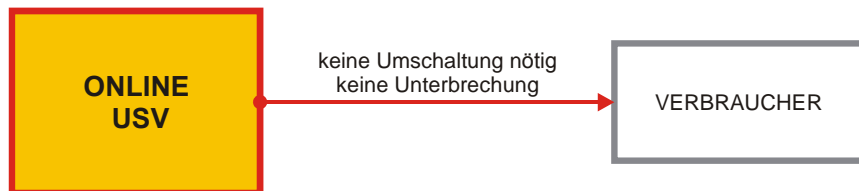
Online-USV

Bei Stromausfall wird die Stromversorgung durch eine Online-USV ohne Unterbrechung weitergeführt.

NETZBETRIEB



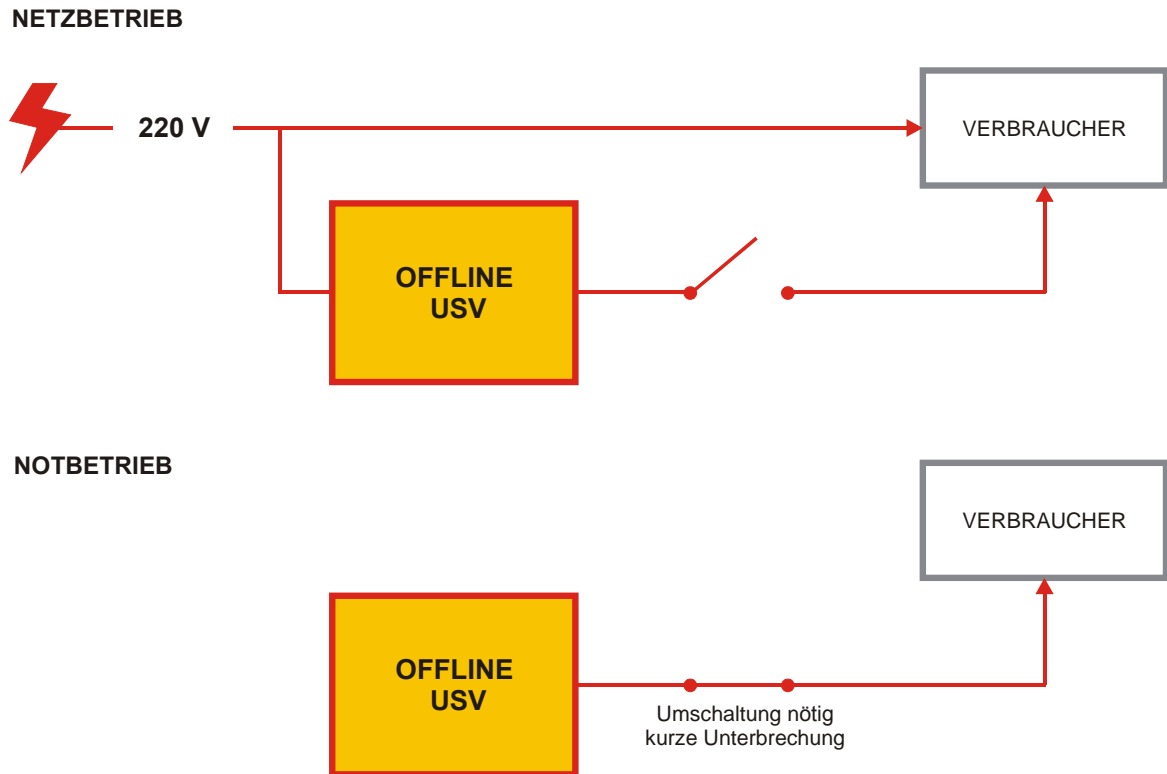
NOTBETRIEB



Grafik Online-USV

Offline-USV

Bei Stromausfall wird die Stromversorgung durch eine Offline-USV mit einer kurzen Umschaltunterbrechung weitergeführt.



Grafik Offline-USV

1.1.5.4 Netzersatzanlagen – NEA

Netzersatzanlagen sind Stromerzeugungseinheiten (ortsfeste oder mobile Notstromaggregate), welche autonom betrieben werden und die Stromversorgung aus dem Netz teilweise oder vollständig ersetzen.

In der Regel haben diese mit Verbrennungsmotoren betriebenen Anlagen Anlaufzeiten bis zu 20 Sekunden. Die Stromversorgung wird bei Netzausfall für diesen Zeitraum unterbrochen.

Die Kombination zwischen USV und NEA ist dann sinnvoll, wenn keine Unterbrechung der Stromzufuhr zulässig ist und die Verbraucher über einen längeren Zeitraum mit Strom versorgt werden müssen.

Zur Sicherstellung der Stromversorgung bei Stromausfällen sind fest eingebaute Notstromaggregate zu empfehlen.

Bei Einsatz von mobilen Notstromaggregaten ist deren Verfügbarkeit sicherzustellen. Dabei sind neben den vertraglichen auch die organisatorischen und technischen Aspekte abzuklären.

Erfahrungsgemäß hat sich gezeigt, dass bei Stromausfall trotz Verträgen und Regelungen Probleme auftreten und die gewünschte Notstromversorgung nicht sichergestellt ist:

- Notstromaggregat wird trotz Vertrag nicht zur Verfügung gestellt (andere Prioritäten)
- Nicht ausreichende Kapazitäten des Notstromaggregates
- Technische Änderungen an Elektroanlage seit dem letzten Probebetrieb
- Techniker für Inbetriebnahme stehen nicht zur Verfügung
- Fehlender Treibstoff

1.2.1 Einführung IKT

Mit dem Sammelbegriff IKT werden alle Strukturen der Informationstechnologie IT und jene der Kommunikationstechnologie KT, welche die Information und Kommunikation in der Gesellschaft sicherstellen, zusammengefasst.

Dazu gehören:

IT

- Computer
- Internet
- Datenleitungen

KT

- Telefonnetze und -anlagen zur Sprachübertragung
- Funkverbindungen

Deshalb wird der Schutz von IKT-Strukturen immer wichtiger. Mit den in diesem Handbuch vorgeschlagenen Maßnahmen und Anleitungen soll die Verfügbarkeit von IKT-Landschaften und deren Sicherheit erhöht werden. Eine hohe Verfügbarkeit bedeutet, dass dem Benutzer sämtliche Dienstleistungen, Informationen und Funktionen eines IKT-Systems zum gewünschten Zeitpunkt zur Verfügung stehen und die Integrität, also die Vollständigkeit und Originalität der Daten sichergestellt ist.

Die steigende Komplexität von IKT-Systemen, hohe Kosten und knappe Budgets, die rasante technische Entwicklung sowie fehlende Ressourcen sind oft Gründe dafür, dass es sehr schwierig ist, ein entsprechendes Sicherheitsniveau zu erreichen und auch zu halten. Der Handlungsdruck, durch aktives IKT-Sicherheitsmanagement das Risiko zu minimieren und allfällige Schäden zu verhindern, steigt immer mehr. Mögliche Schäden sind einerseits wirtschaftlicher Art, andererseits können gerade im Bereich von Behörden und Organisationen mit Sicherheitsaufgaben bei IKT-Ausfällen auch die Sicherheit und das Leben von Menschen gefährdet werden.

Einige der wichtigsten Erfolgsfaktoren im IKT-Sicherheitsmanagement sind aber nicht nur hohe Investitionen in die Sicherheitstechnik oder ausschließlich fachlich hoch qualifiziertes Personal, sondern ein weiterer Humanfaktor: Zuverlässige und gut informierte Mitarbeiter, gesunder Menschenverstand und gute organisatorische Regelungen.

Ein erreichter Sicherheitsstandard in der IKT ist jedoch auch ständigen Anpassungen und Verbesserungen unterworfen und stellt einen ständigen Prozess dar. Dabei müssen sich die Verantwortlichen immer wieder dieselben Fragen stellen:

- Folgen eines IKT-Ausfalles über einen längeren Zeitraum (Fortsetzung der Arbeit, Schadenshöhe)
- Folgen von Datenverlust oder -veränderung (auch durch Dritte)
- Folgen von Missbrauch von Daten und Informationen

Aber auch durch Aussagen wie:

„Wir betreiben ein sicheres Netz.“, „Bei uns gibt es keine geheimen Daten zu holen.“, „Wir vertrauen in unsere Mitarbeiter.“, oder „So etwas ist bei uns noch nie passiert.“ wird der eigene Schutzbedarf oft unterschätzt.

Die Umsetzung eines IKT-Sicherheitskonzeptes bringt nicht nur einen Sicherheitsgewinn, sondern auch Wettbewerbsvorteile, eine Steigerung der Arbeitsqualität sowie die Effizienz der Tätigkeit des eingesetzten IKT-Personals.

1.2.2 Ausfallszenario

Das Ausfallszenario bei einem IKT-Problem kann sehr vielfältig sein. Beispielhaft sind nachstehend einige mögliche Szenarien angeführt und in weiterer Folge vier in der Praxis aufgetretene Fälle beschrieben.

Ein funktionierendes IT-Sicherheitsmanagement setzt auch ein funktionierendes Backup-Management voraus. Durch unregelmäßige Durchführung von Datensicherungen sowie durch Sicherungen auf möglicherweise defekte Datensicherungsmedien können enorme Datenverluste entstehen. Die Sicherungen sollten auch an mehreren verschiedenen Sicherungsplätzen verwahrt werden. Hier bieten sich Server in anderen Gebäuden, die Lagerung von externen Festplatten außerhalb von Betriebsgebäuden, etc. an.

Die Verwendung von Antiviren-Programmen ist aus der IKT-Sicherheit nicht mehr wegzudenken. Allerdings hinkt jede Antiviren-Software den aktuellen Entwicklungen in diesem Bereich nach. Deshalb ist es notwendig, diese Software auch regelmäßig, unter Umständen auch täglich upzudaten. Dabei dürfen aber sogenannte IT-Inseln wie Laptops, die nur unregelmäßig im Netz integriert sind, nicht vergessen werden.

Immer wieder gelingt es Hackern, mit gezielten Angriffen die aufwendigsten Sicherheitsvorkehrungen von IKT-Einrichtungen zu überwinden und Daten zu lesen, zu verändern oder zu stehlen. Hier bieten sich verschiedene Lösungsansätze: Internetzugänge mit entsprechenden Sicherungssystemen abzusichern, ein entsprechendes Backup-Management einzurichten, aber auch vertrauliche Daten nochmals zu verschlüsseln.

Durch den Ausfall von Schlüsselpersonal oder Administratoren aus dem Bereich IKT können gravierende Folgen entstehen. Hier ist es notwendig, entsprechende Systemeinstellungen und Parameter genau zu dokumentieren, Passwörter zu hinterlegen und Vertretungsregeln einzurichten. Weiters sollte ein einfacher, von jedermann abarbeitbarer Notfallplan mit Anweisungen für die Verfahrensweise bei den wichtigsten Schadensfällen erstellt werden.

Immer wieder kommt es vor, dass betriebseigene Personen IKT-Landschaften manipulieren oder Daten an Dritte weitergeben. Hier gilt es wieder, diverse Räumlichkeiten gegen unbefugten Zutritt zu sichern, mit entsprechenden Überwachungssystemen Zugriffe zu überwachen und gegebenenfalls auch vertrauliche Daten zu verschlüsseln.

Ausfall von Bankomaten am 30.10.2005

In weiten Teilen Österreichs gab es am Sonntag, 30.10.2005 große Probleme mit vielen Bankomaten und Bankomatkassen. Laut der technischen Betreuerfirma der Bankomaten APSS kam es durch ein technisches Problem zu einem Ausfall der Kommunikation zwischen Bankomaten und dem Rechenzentrum. Von diesem Ausfall waren ca. 400 der österreichweit 4.000 Bankomaten betroffen.

Ausfall der Telefonanlage in einem Krankenhaus in Eisenstadt

Teile von Eisenstadt waren am 07.08.2007 von einem Stromausfall betroffen. Bohrarbeiten führten zu einer Störung von Hochspannungskabeln. Betroffen vom Stromausfall war unter anderem auch ein Krankenhaus. Das Spital wurde zwar mit Notstrom versorgt, jedoch fiel in diesem Zeitraum die Telefonanlage aus. Das Krankenhaus war für ca. 2 Stunden nur über Mobiltelefone erreichbar.

Ausfall des A1-Breitbandes am 16.01.2008

Am 16.01.2008 fiel im Zeitraum zwischen 21:00 und 01:00 Uhr das Breitbandangebot von A1 in Niederösterreich aus. Grund dafür war ein Leitungsproblem bei der Mobilkom-Mutter Telekom. Auch das redundante System konnte den Ausfall nicht auffangen. Weiters litt die Sprachqualität am GSM-Netz in diesem Zeitraum in Gesamtösterreich.

Angriffe mit Schadsoftware

Ende Jänner 2008 meldete Trendmicro (Hersteller von Antiviren-Software) das Auftreten einer Welle von Attacken, die offensichtlich gegen Exiltibeter gerichtet waren. Auffallend war dabei der Zusammenhang mit dem Aufstand der Mönche in Tibet. Durchgeführt wurden dabei gezielte Angriffe mittels bis dahin unbekanntem Trojanern, die eine bis dahin unbekannte Sicherheitslücke ausnutzten. Mit derartigen Angriffen kann großer Schaden angerichtet werden. Neben Diebstahl von Informationen können auch gezielt Webseiten gecrackt, Systeme gestört und außer Funktion genommen werden.

1.2.3 Auswirkungen für Verbraucher

Der Zusammenbruch der IKT-Versorgung kann gravierende Auswirkungen nach sich ziehen. Ausfälle von Kommunikationseinrichtungen, wie z.B. von Anlagen der nationalen Telefongesellschaft (Backbone Telekom Austria) haben nicht nur Ausfälle der Festnetz- und Mobiltelefonie, sondern auch des Internets zur Folge.

Die Auswirkungen für den privaten, gewerblichen oder behördlichen Verbraucher unterscheiden sich nach Schweregrad und Umfang der Störung:

1. Einzelausfälle interner IKT Strukturen von Privaten, Betrieben, Behörden oder Einrichtungen
 - IT, KT Strukturen einer Einrichtung fallen aus. Datenverarbeitung und/ oder Telefonie sind betroffen. Die Einrichtung ist telefonisch nicht erreichbar, IT Verbindungen sind tot und Datenaustausch ist nicht mehr möglich, die interne Datenverarbeitung fällt aus.
2. Ausfälle einzelner IKT-Anbieter
 - Es kommt zu Ausfällen eines Anbieters im Bereich der Mobiltelefonie oder des Festnetzes oder zu Ausfällen einzelner Internetdienstleister, Web-Seiten sind nicht erreichbar, E-Mail fällt aus, Rechenzentren können nicht mehr genutzt werden. Betroffen sind alle Nutzer des betroffenen Dienstleisters an vielen Standorten.
3. Ausfall von Netzbereichen
 - IKT-Strukturen auf Orts- oder Bezirksebene brechen zusammen. Betroffen sind alle privaten, gewerblichen und öffentlichen Nutzer der ausgefallenen Einrichtung in einem geografisch abgegrenzten Bereich.
4. Großflächiger Zusammenbruch von IKT-Strukturen
 - Telefonie und/oder IT-Verbindungen fallen auf Landes-, Bundes- oder internationaler Ebene großflächig aus.
 - Worst Case (schlechteste oder ungünstigste) Situation – alle Nutzer von IKT-Einrichtungen in großen Bereichen sind betroffen.

IKT-Ausfälle können in der Praxis folgende Auswirkungen haben:

Informationstechnologie

- Überwachungsanlagen können Alarme nicht mehr weiterleiten
- Durch Ausfall von Sicherheits-, Steuer- und Kontrollsystemen kann es zu Fehlfunktionen und damit zu Unfällen kommen.
- Untersuchungen und Behandlungen in Krankenhäusern mit lebensrettenden IT-gestützten medizintechnischen Geräten können eingeschränkt oder überhaupt nicht mehr möglich sein
- Unternehmen, Versorgungseinrichtungen, Transportdienste wie Bahn, Luftfahrt, Autobahnen, Banken, öffentliche Verwaltungen und Behörden können ihre Aufgabe teilweise oder vollständig nicht mehr erfüllen. Die Folgen:
 - Beeinträchtigung der öffentlichen Sicherheit
 - Störungen/Ausfall der Versorgung mit lebenswichtigen Gütern
 - Störungen/Ausfälle/Zusammenbruch des Transportwesens für Mensch und Güter
 - Störungen/Ausfälle/Zusammenbruch des Banken- und Finanzwesens
 - Bargeldknappheit/Bezahlung über Bankomat oder Kreditkarte nicht mehr möglich
 - Produktionsausfälle und schwere Schäden in Landwirtschaft, Industrie, Gewerbe und Tourismus

Kommunikationstechnologie

- Notrufe können nicht mehr getätigt werden
- Notarzt, Feuerwehr, Polizei und andere Hilfsdienste können nicht mehr rechtzeitig eingreifen, dadurch schwerste Auswirkungen auf Menschen und Sachen möglich
- Der Austausch von Informationen zwischen Krankenhäusern und Expertendiensten, z.B. Vergiftungszentrale funktioniert nicht mehr
- Die Kommunikation über Telefon und Telefax fällt aus.
Informationen können nicht rechtzeitig gegeben oder eingeholt werden, dadurch massive Beeinträchtigung von üblichen Abläufen, der Sicherheit und hohe wirtschaftliche Schäden in allen Bereichen
- Bei Ausfall des Festnetzes und der Mobiltelefone können auch die Partner im Zivil- und Katastrophenschutz das gängigste und am weitesten verbreitete Kommunikationsmittel nicht mehr nutzen. Dadurch können weitere Verzögerungen in der Bewältigung der Notlage eintreten.

1.2.4 IKT in Tirol

1.2.4.1 Gesetzliche Grundlagen

Datenschutzrichtlinie

Richtlinie 95/46/EG des europäischen Parlamentes und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

Internationaler Datenverkehr

Rat und Europäisches Parlament haben die Kommission ermächtigt, auf der Grundlage von Artikel 25(6) der Richtlinie 95/46/EG zu entscheiden, ob ein Drittstaat aufgrund von internen Rechtsvorschriften oder eingegangenen internationalen Verpflichtungen ein angemessenes Schutzniveau gewährleistet.

Telekom-Datenschutzrichtlinie

Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

Datenschutzverordnung der EU-Organe

Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr.

E-Commerce-Richtlinie

Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“).

Datenschutzgesetz

Das Datenschutzgesetz 2000 (DSG 2000, Bundesgesetz über den Schutz personenbezogener Daten), BGBl. I Nr. 165/1999 idF. BGBl. I Nr. 13/2005, ist das geltende österreichische Datenschutzgesetz, und damit die wichtigste Rechtsvorschrift zum Datenschutz in Österreich.

E-Government-Gesetz

10. Bundesgesetz, mit dem ein E-Government-Gesetz erlassen wird, sowie das Allgemeine Verwaltungsverfahrensgesetz 1991, das Zustellgesetz, das Gebührengesetz 1957, das Meldegesetz 1991 und das Vereinsgesetz 2002 geändert werden (BGBl. Nr. 10/2004).

§ 1. (1) Dieses Bundesgesetz dient der Förderung rechtserheblicher elektronischer Kommunikation. Der elektronische Verkehr mit öffentlichen Stellen soll unter Berücksichtigung grundsätzlicher Wahlfreiheit zwischen Kommunikationsarten für Anbringen an diese Stellen erleichtert werden.

(2) Gegen Gefahren, die mit einem verstärkten Einsatz der automationsunterstützten Datenverarbeitung zur Erreichung der in Abs. 1 genannten Ziele verbunden sind, sollen zur Verbesserung des Rechtsschutzes besondere technische Mittel geschaffen werden, die dort einzusetzen sind, wo nicht durch andere Vorkehrungen bereits ausreichender Schutz bewirkt wird.

Informationssicherheitsgesetz

Bundesgesetz über die Umsetzung völkerrechtlicher Verpflichtungen zur sicheren Verwendung von Informationen (Informationssicherheitsgesetz, InfoSiG) BGBl. I Nr. 23/2002 idF: BGBl. I Nr. 129/2003 idF: BGBl. I Nr. 10/2006:

Ziel des Gesetzes ist die Umsetzung völkerrechtlicher Verpflichtungen Österreichs zur sicheren Verwendung von klassifizierten Informationen, unabhängig von Darstellungsform und Datenträger, im Bereich der Dienststellen des Bundes.

Telekommunikationsgesetz 2003

Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 – TKG 2003), BGBl. I Nr. 70/2003 idF: BGBl. I Nr. 178/2004 idF: BGBl. I Nr. 133/2005.

§ 1. (1) Zweck dieses Bundesgesetzes ist es, durch Förderung des Wettbewerbes im Bereich der elektronischen Kommunikation die Versorgung der Bevölkerung und der Wirtschaft mit zuverlässigen, preiswerten, hochwertigen und innovativen Kommunikationsdienstleistungen zu gewährleisten.

Weitere gesetzliche Bestimmungen

Weitere einzelne Bestimmungen aus Gesetzen mit Bezug zum Datenschutz finden sich in der nachstehenden Aufstellung:

Allgemeines Bürgerliches Gesetzbuch (ABGB), JGS Nr. 946/1811

Allgemeines Verwaltungsverfahrensgesetz 1991 (AVG), BGBl. Nr. 51

Bundesgesetz über das Bundesgesetzblatt 1996, BGBl. Nr. 660

Art. 8 Bundes-Verfassungsgesetz (B-VG)

E-Commerce-Gesetz (ECG), BGBl. I Nr. 152/2001

Exekutionsordnung, RGBl. Nr. 79/1896

Gentechnikgesetz, BGBl. Nr. 510/1994

Gerichtsorganisationsgesetz, RGBl. Nr. 217/1896

Konsumentenschutzgesetz, BGBl. Nr. 140/1979

Mediengesetz, BGBl. Nr. 314/1981

Meldegesezt 1991, BGBl. Nr. 9/1992

Strafgesetzbuch, BGBl. Nr. 60/1974

Strafprozessordnung 1975, BGBl. Nr. 631

Versicherungsvertragsgesetz 1958, BGBl. Nr. 2/1959

Verwaltungsstrafgesetz 1991, BGBl. Nr. 52

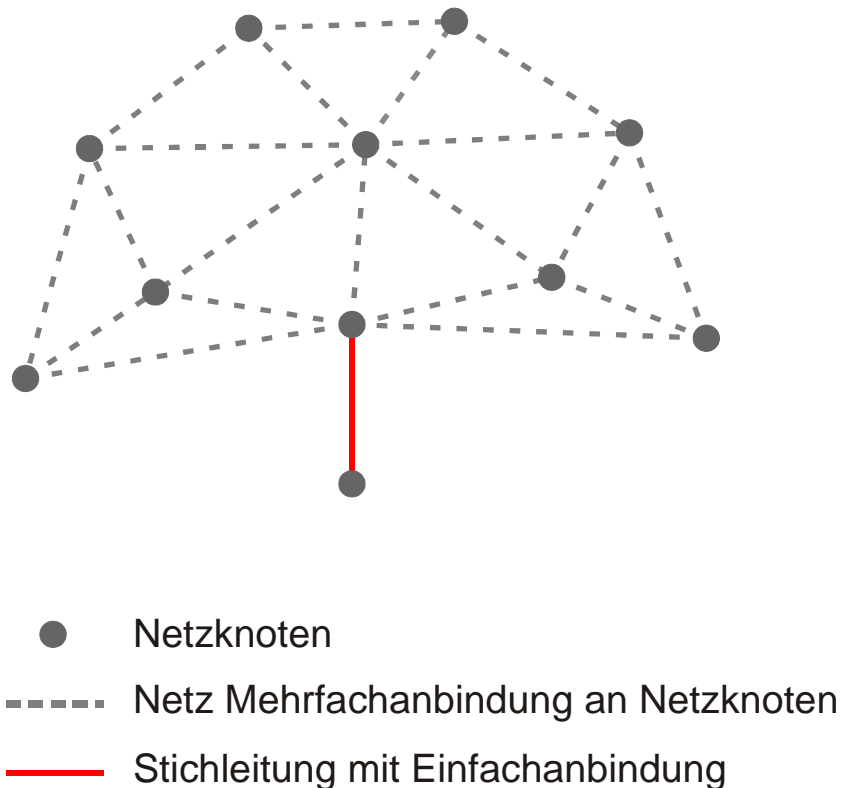
Zivilprozessordnung, RGBl. Nr. 113/1895

1.2.4.2 Architektur IKT-Netz

IKT-Verbindungen sind als Netze konzipiert und aufgebaut. Das Netz mit Netzknoten und Mehrfachanbindungen garantiert auch bei Unterbrechungen an einzelnen Stellen eine hohe Funktionssicherheit.

Die Funktionssicherheit eines Netzes hat zur Entwicklung des Internets beim amerikanischen Militär geführt. Ziel des amerikanischen Militärs war es, bei Atomschlägen in Amerika, durch Einsatz der Netztechnik die Ausfälle der Kommunikationsnetze im Rahmen zu halten und damit Totalausfälle zu verhindern.

In der Praxis gibt es eine große Vermischung zwischen den IT- und den KT-Netzen. So werden Verbindungen der Informationstechnologie wie Internet, Datenleitungen, usw. über die gleichen Kabel oder Funkstrecken geführt wie jene der Kommunikationstechnologien. Im alpinen Raum in den Seitentälern sind noch vielfach die Leitungen nicht in Netzen verbunden. Leitungen, welche nur an einer Stelle mit dem Netz verbunden sind, werden als Stichleitungen bezeichnet und sind aufgrund dessen nicht ausfallssicher.



Symbol-Grafik Architektur IKT-Netz

1.2.4.3 Telekom Austria – internationale Anbindung

Die Telekom Austria ist der mit großem Abstand wichtigste Betreiber von IKT-Netzinfrastruktur in Österreich. Das österreichische IKT-Netz ist über große leistungsfähige Verbindungen (Lichtwellenleiter), den Telekom Austria JetStream, mehrfach an die internationalen IKT-Netze angebunden.



Grafik Telekom Austria JetStream

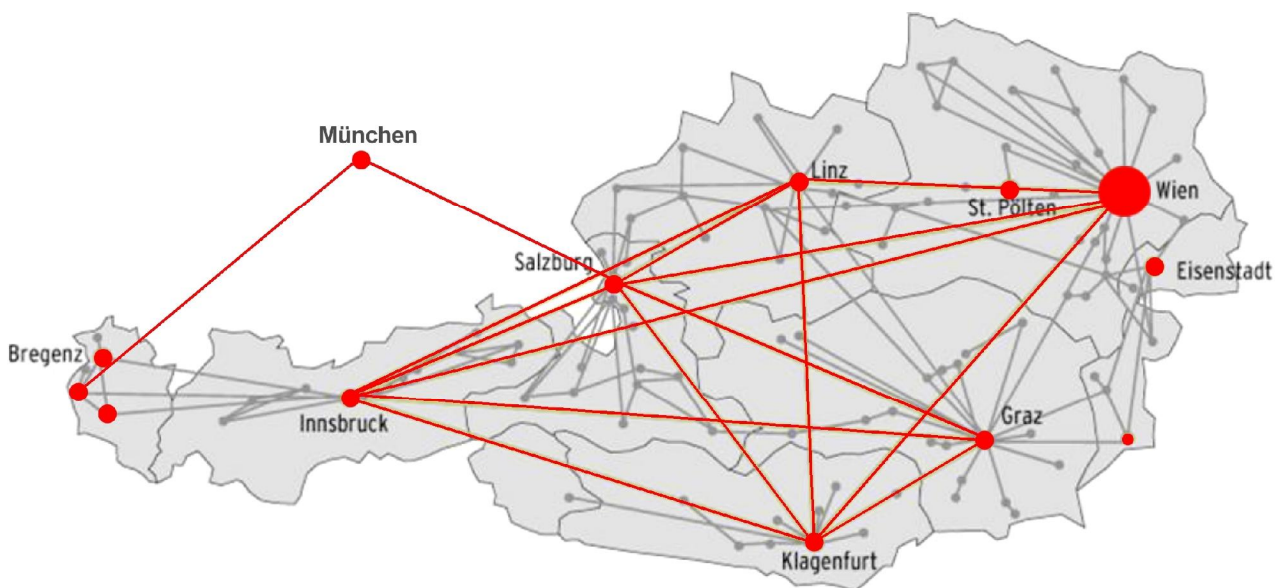
(Quelle: Telekom Austria, Stand 2007)

1.2.4.4 Telekom Austria – IKT-Netz Österreich

Die Telekom Austria betreibt mit dem Backbone die dichteste und flächendeckende IKT-Netzinfrastruktur in Österreich.

Über den Backbone werden Festnetztelefonie, Mobiltelefonie und Datenübertragungen aller Art von mehreren Anbietern abgewickelt .

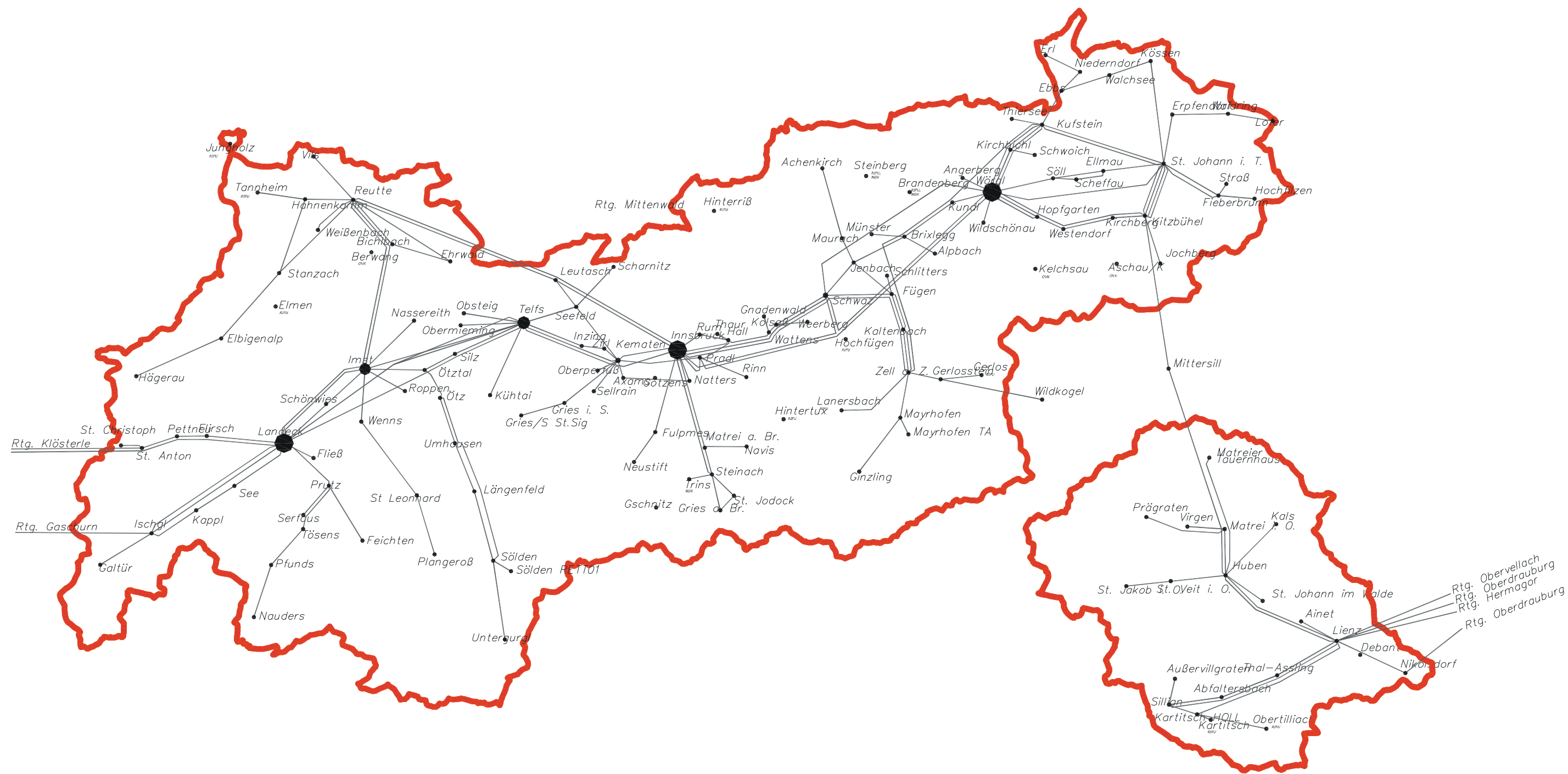
Ein kompletter Ausfall dieses Netzes legt, aufgrund von Recherchen, fast die gesamte Telekommunikation und Datenübertragung in Österreich lahm. Ausnahmen bilden von diesem Netz komplett getrennt geführte Datenübertragungen, wie z.B. die Datenübertragung zur Steuerung von Kraftwerken.



Grafik Backbone Österreich

(Quelle: Telekom Austria, Stand 2007)

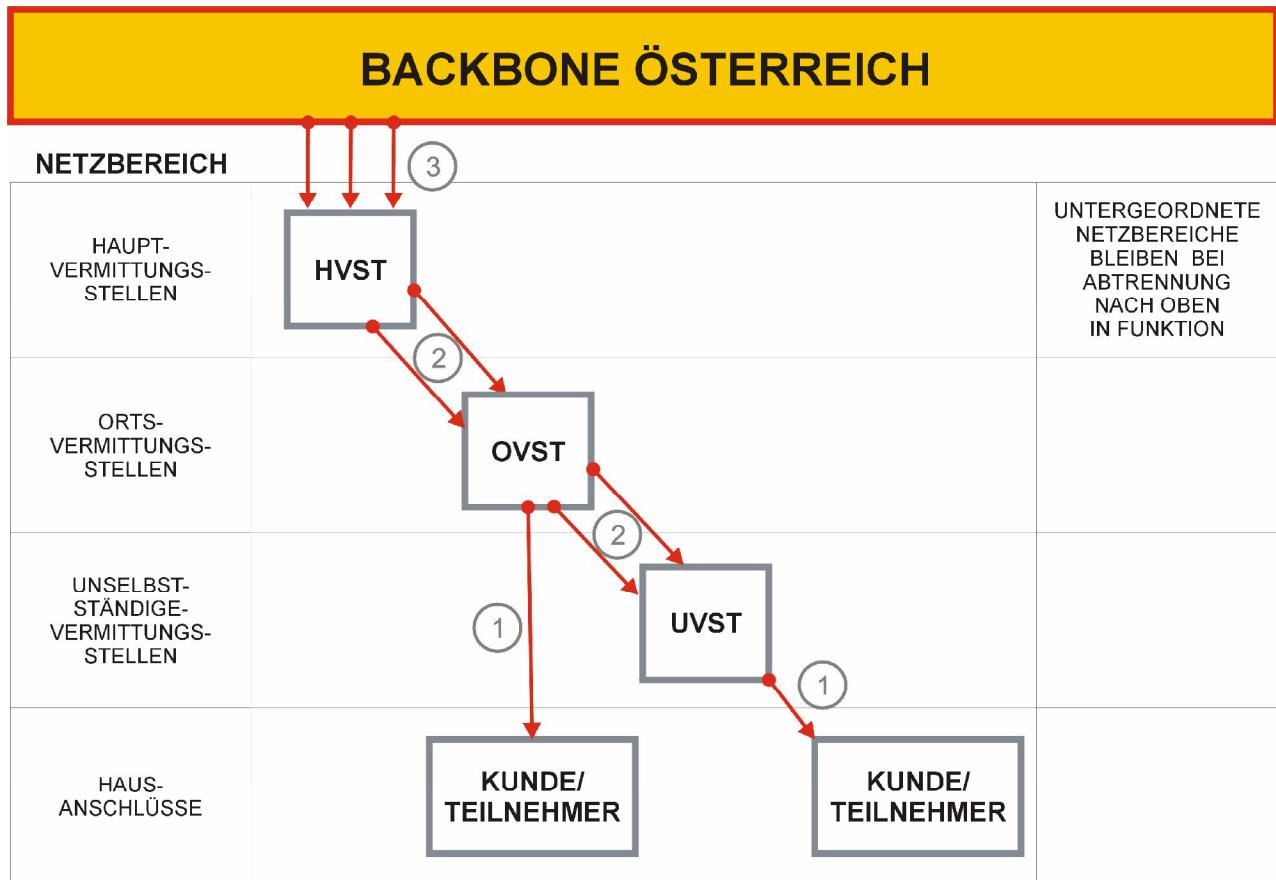
1.2.4.5 Telekom Austria – Backbone in Tirol



Grafik Telekom Austria – Backbone Tirol

(Quelle: Telekom Austria, Stand 2007)

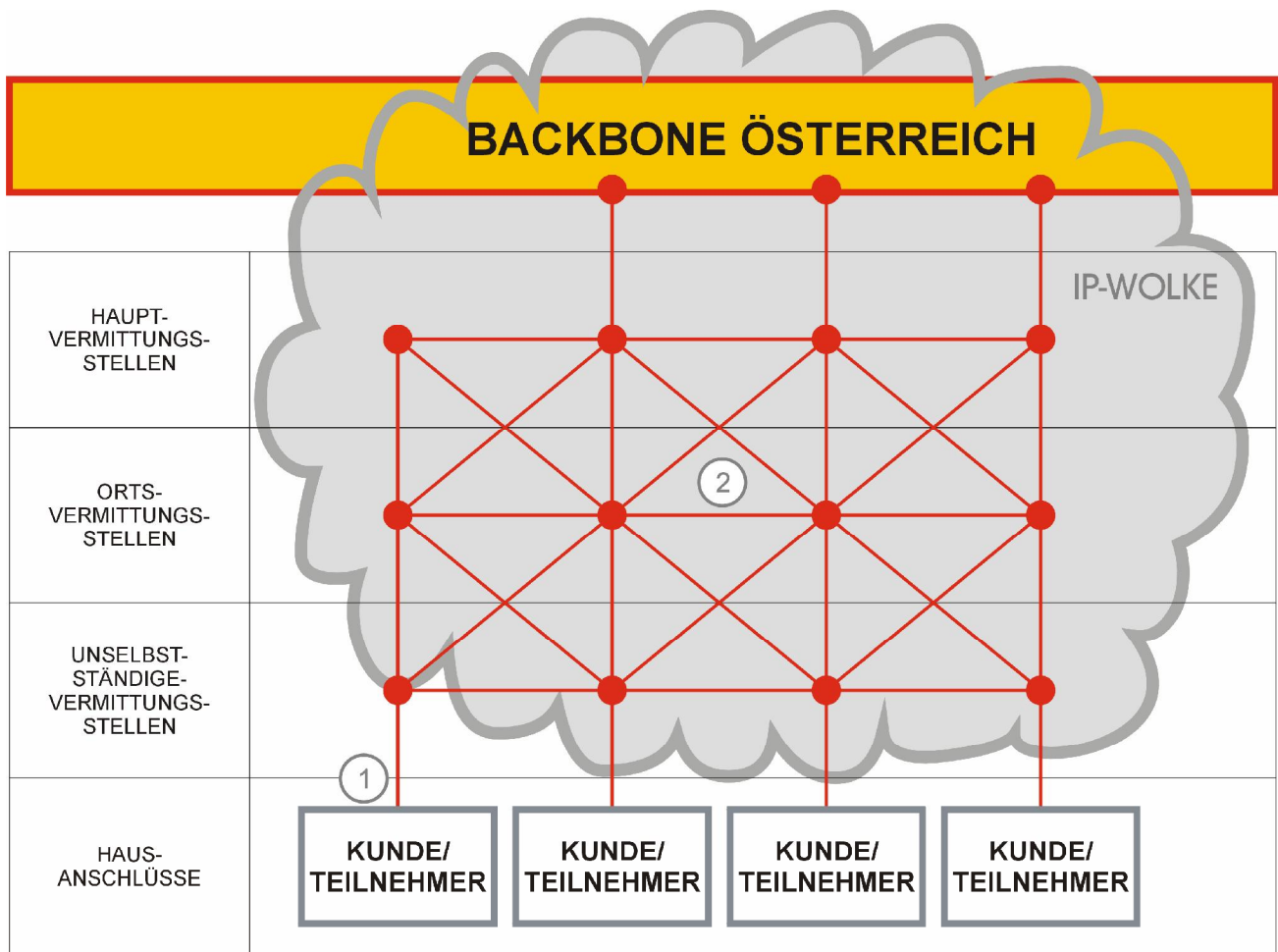
1.2.4.6 Architektur Technologieplattform für Telefon- und Sprachübertragung
KT-Netz in Tirol



- ① EINFACHE ANBINDUNG (1 LEITUNG)
- ② REDUNDANTE ANBINDUNG (2 LEITUNGEN)
- ③ MEHRFACH REDUNDANTE ANBINDUNG (MEHRERE LEITUNGEN)

Grafik Architektur Technologieplattform für Telefon- und Sprachübertragung KT-Netz in Tirol

1.2.4.7 Architektur Technologieplattform für Datenübertragung IT(IP)-Netz in Tirol



- ① EINFACHE ANBINDUNG (1 LEITUNG)
- ② IN IP-WOLKE: MEHRFACH REDUNDANTE ANBINDUNG (MEHRERE LEITUNGEN)

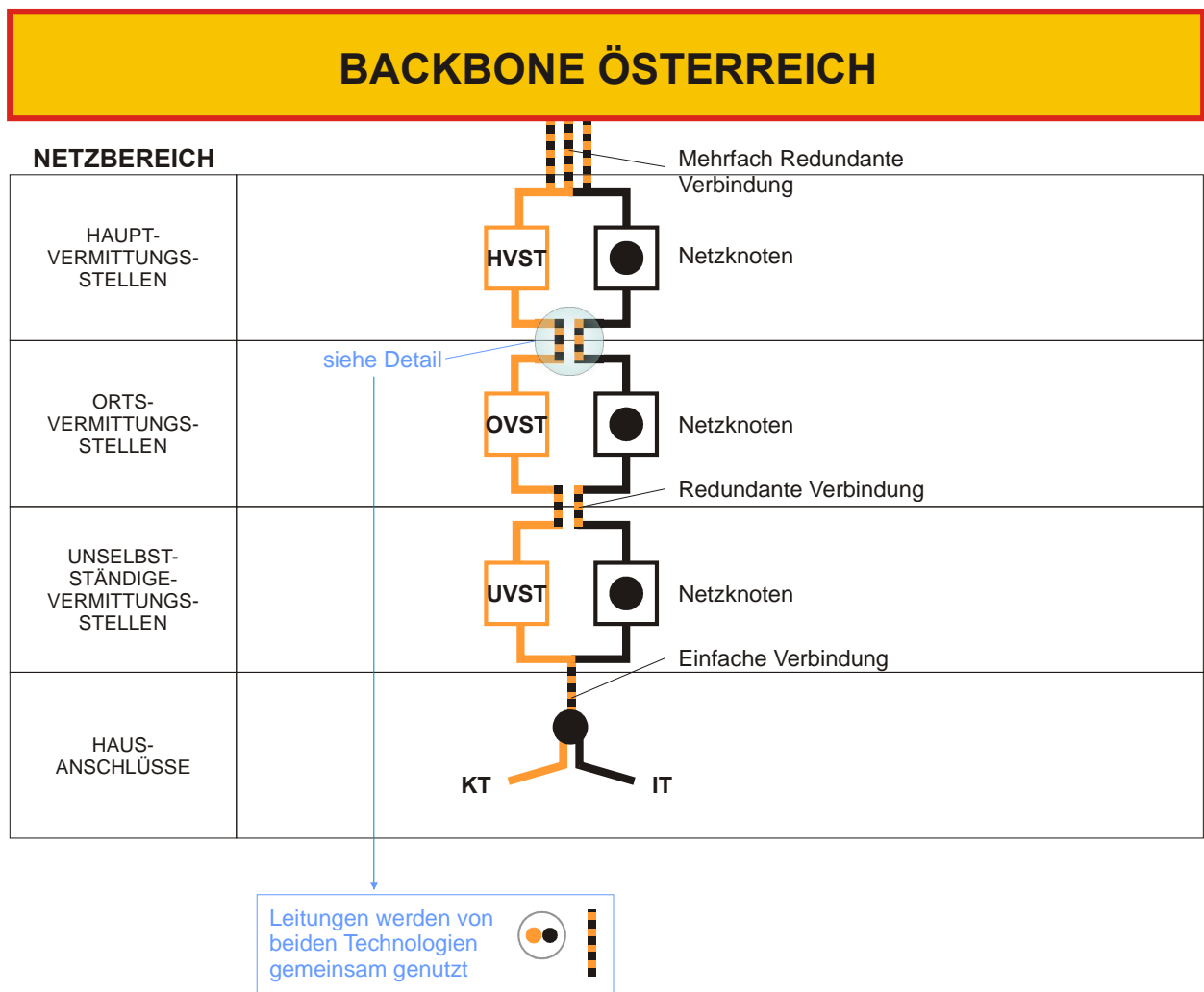
Grafik Architektur Technologieplattform für Datenübertragung IT-Netz in Tirol

1.2.4.8 Anwendung der Technologieplattformen auf der physikalischen Infrastruktur

Auf dem Festnetz, d.h. der physikalischen Infrastruktur der Telekom Austria, werden zwei unterschiedliche Technologieplattformen betrieben:

1. Plattform für Telefon- und Sprachübertragung – KT Kommunikationstechnologie
2. Plattform für Datenübertragung – IT Informationstechnologie

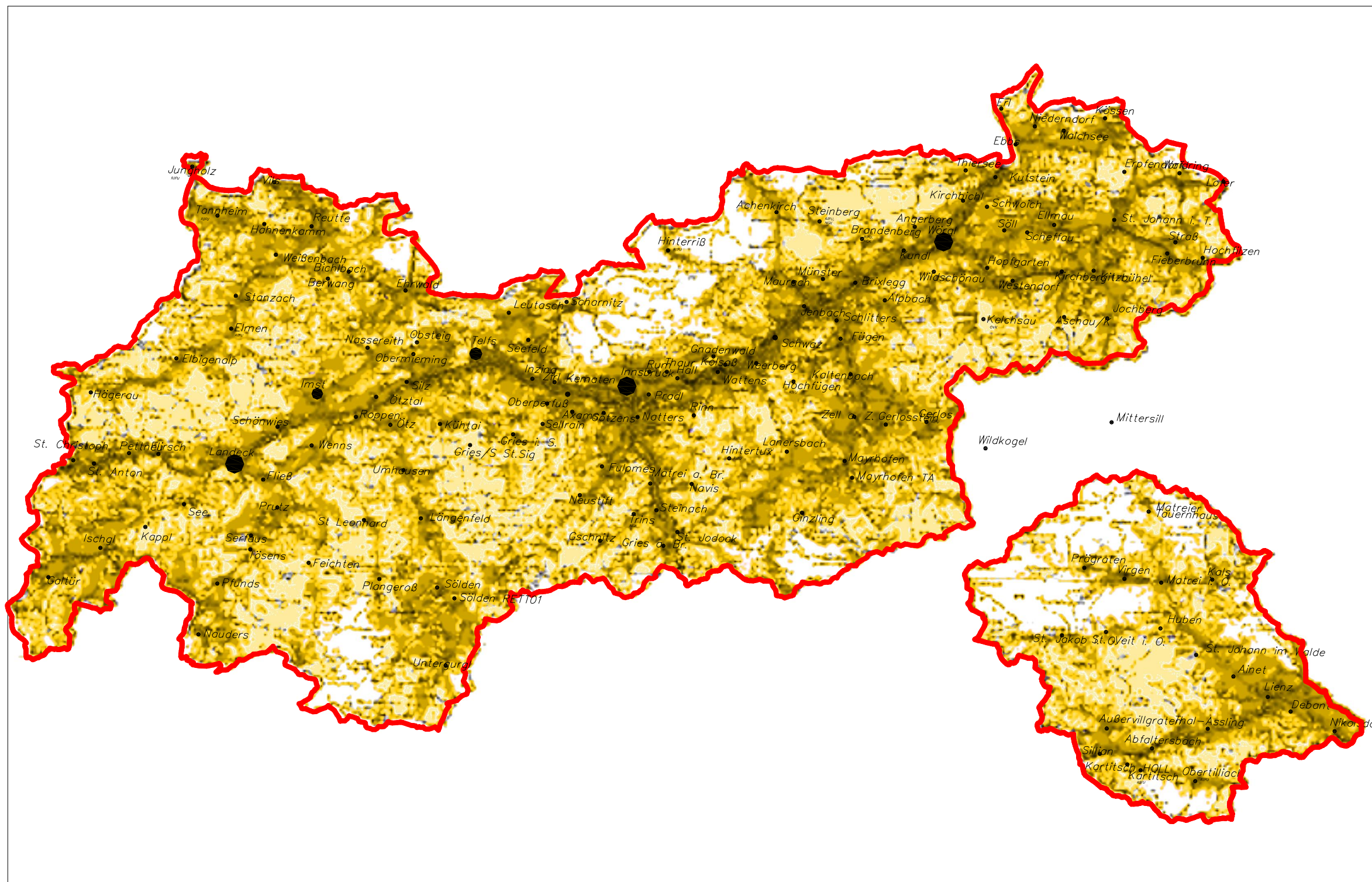
Gemeinsam genutzt werden dabei die Leitungen. In den Vermittlungsstellen bzw. Netzknoten sind beide Technologien getrennt. Das bedeutet, dass bei einem technologiebedingten Ausfall der Kommunikationstechnologie die Informationstechnologie in Funktion bleibt und umgekehrt. Eine Unterbrechung der Leitungen bedeutet den Ausfall beider Technologien.



Grafik Technologieplattformen auf der physikalischen Infrastruktur

1.2.4.9 Mobilkom Austria – GSM Abdeckung in Tirol

In einem gebirgig strukturierten Land wie Tirol ist die vollständige Abdeckung mit Mobiltelefonie schwierig. In den farblich gekennzeichneten Zonen ist in Tirol die Abdeckung mit Mobiltelefonie GSM / GPRS gewährleistet.



Grafik GSM / GPRS Abdeckung in Tirol

(Quelle: Mobilkom Austria, Stand 2007)

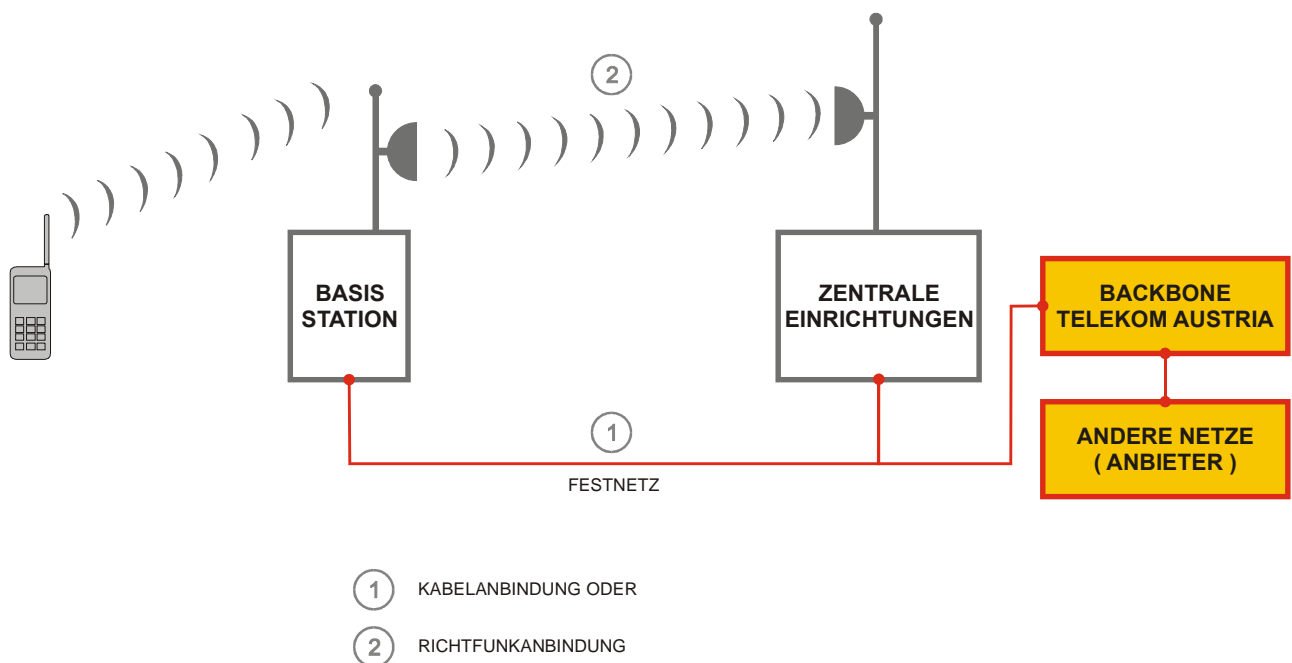
1.2.4.10 Mobiltelefonie in Tirol

Netzinfrastrukturen

Die wesentlichen Elemente des Mobilfunknetzes sind:

1. Die Basisstationen
Sie stellen die Schnittstelle zu den Handys dar
2. Die zentralen Einrichtungen
Sie sind mit „Intelligenz“ ausgestattet und stellen die Verbindung in das Festnetz und zu anderen Netzen her.

Basisstationen sind in der Regel über das Telefonfestnetz oder über Richtfunkstrecken mit den Zentralen Einrichtungen verbunden.



Grafik: Architektur Mobiltelefonnetz

Eigene Netze werden von den Anbietern A1-Mobilkom, T-mobile, ONE und „Drei“ betrieben. Alle anderen Anbieter betreiben ihre Dienste über diese Strukturen.

Verhalten der Mobiltelefonanlagen bei Stromausfall

Basiszellen sind großteils mit Batterien notstromversorgt. Bei Stromausfall reicht ihre Kapazität je nach Gesprächsaufkommen für 30 – 60 Minuten. Danach funktionieren Sie nicht mehr bis die Netzstromversorgung wieder hergestellt wird.

Die Notstromversorgung der Zentralen Einrichtungen wird mittels Batterieanlagen (USV) und fest eingebauten Notstromaggregaten sichergestellt. Die USV stellt einen unterbrechungsfreien Übergang zwischen der Stromversorgung aus dem Netz und dem Anlaufen des Dieselaggregates sicher. Das Dieselaggregat kann 70 Stunden autonom ohne Nachtanken betrieben werden. Bei Ausfall des Notstromaggregates reicht die Kapazität der Batterieanlage für 3 Stunden. Der größte Netzbetreiber, A1 Mobilkom kann innerhalb dieser Zeit ein konzerneigenes fahrbares Notstromaggregat anschließen. Die fahrbaren Aggregate werden in Innsbruck vorgehalten.

A1 Mobilkom verfügt auch über ein ausgereiftes Krisenmanagementkonzept und ist in der Lage, ausgefallene Zellen mit mobilen Containern zu ersetzen. Diese können via Hubschrauber auch im schwierigen Gelände zum Einsatz gebracht werden.

Ein intaktes Festtelefonnetz ist die Voraussetzung für das Funktionieren der Mobilfunktelefonie. Fällt die Verbindung zwischen Basisstation und der Zentralen Einrichtung aus, können im Bereich der Basisstation keine Gespräche mehr geführt werden. Ist diese intakt, jedoch die Verbindung von der Zentralen Einrichtung in das Festnetz unterbrochen, können Teilnehmer innerhalb des Sendebereiches der Basisstation und der Zentralen Einrichtung untereinander sprechen. Eine Verbindung nach außen ist nicht möglich.

Ein Zusammenbruch des Festnetzes führt zu weitestgehenden Ausfällen der Mobiltelefonie. Ausnahmen bilden dabei jene Basisstationen und Zentralen Einrichtungen, welche über Funkstrecken miteinander verbunden sind. Gespräche sind in diesen Fall nur unter Teilnehmern aus dem direkten Sendebereich beider Einrichtungen möglich.

1.2.4.11 Digitalfunk BOS Austria – Tirol

Zweck

Das digitale Funknetz BOS Austria – Tirol ermöglicht die Kommunikation auf Sprach- und Datenebene zwischen den teilnehmenden Behörden und Organisationen mit Sicherheitsaufgaben (BOS). Dabei ist die gleichzeitige Übertragung von Sprache und Daten in hoher Qualität, die Kommunikation zwischen einzelnen Teilnehmern, in Gruppen und parallel zwischen mehreren Gruppen möglich. Neben den Behörden und Organisationen mit Sicherheitsaufgaben (BOS) wie Polizei, Rettung, Feuerwehr, Berg- und Wasserrettung usw. sind die Einsatzleitungen auf Landes-, Bezirks- und Gemeindeebene, die Krankenhäuser und Einrichtungen wie der Flughafen Innsbruck sowie die Leitstelle Tirol über dieses System erreichbar.

Netzinfrastrukturen

Funkbasisstationen

Die Netzinfrastruktur besteht in Tirol derzeit aus 184, im Endausbau aus 190 Funkbasisstationen und 14 Tunnelbasisstationen mit Sende- und Empfangseinrichtungen.

Verbindungsnetzwerk

Die Funkbasisstationen sind über das Verbindungsnetzwerk des Bundesministeriums für Inneres (BMI) und dessen Vertragspartner Telekom Austria via Kabel oder Richtfunkanbindung mit dem Main Switching Office (MSO) in Hall in Tirol verbunden.

Main Switching Office – MSO

Das MSO in Hall wird vom BMI betrieben. Es ist die „Hauptvermittlungsstelle“ des Digitalfunknetzes BOS Austria – Tirol. Alle Gespräche und Datenübertragungen, welche über den Sendebereich einer Funkbasisstation hinausgehen, müssen über das MSO geführt werden.

Endgeräte

Für die Sprachübertragung kommen Fixstationen in Gebäuden, fest eingebaute Mobilfunkgeräte in Fahrzeugen und Handfunkgeräte zum Einsatz.

Verhalten der Digitalfunkanlagen bei Stromausfall

Funkbasisstationen

Die Basisstationen sind mittels USV notstromversorgt. Die Kapazität der Batterien stellt eine Betriebszeit ohne Netzstrom von > 24 Stunden sicher. Jede der Sendeanlagen ist mit einem Anschluss für ein mobiles Notstromaggregat versehen. Die Feuerwehren sind für die Notstromversorgung der Sendeanlagen geschult und verfügen über die notwendigen Geräte.

Fällt eine Funkbasisstation total aus, so können die Funkgeräte auf Direct Mode Operation (DMO) umgeschaltet und weiterbetrieben werden. Allerdings ist nur noch eine direkte Kommunikation von Gerät zu Gerät mit eingeschränkter Reichweite möglich.

Verbindungsnetzwerk ATM

Die Funkbasisstationen sind über Kabel und Funkanbindung mit dem Main Switching Office (MSO, Hauptvermittlungsstelle des BOS-Netzes in Tirol) des BMI in Hall verbunden. Jede Sprach- und Datenverbindung innerhalb einer Funkbasisstation oder auch zwischen Funkbasisstationen wird über die „Hauptvermittlungsstelle“ geführt.

Dabei bedient sich das Innenministerium der Infrastrukturen der Telekom. Für das Verbindungsnetzwerk garantiert die Telekom Austria einen autarken Betrieb von 10 Stunden nach einem Stromausfall.

Bei Störungen im Telekomnetz ist ein „Umrouting“ (Umleitung) durch das Netzwerkmanagement des BMI über das innenministeriumseigene Netzwerk ATM (Asynchronous Transfer Mode) oder ISDN Verbindungen der Telekom möglich. Das ATM Netzwerk des Innenministeriums bedient sich zwar der Leitungen der Telekom, verfügt aber über eigene Switches und Router (Schaltstellen). Eine Umleitung kann theoretisch bis zur Nebenstelle bei der nächstgelegenen Polizeidienststelle vor der Funkbasisstation geschaltet werden. Die Telekom führt doppelte Leitungen, (in den Seitentälern meist im gleichen Rohr) bis zu den Vermittlungsstellen. Von dort führt eine Leitung zu den Hausanschlüssen oder der Nebenstelle der Polizei. Bei Unterbrechung der einfachen Leitung im letzten Abschnitt gibt es keine Umleitungsmöglichkeit.

Bei Ausfall des Verbindungsnetzwerkes oder einer Unterbrechung der Verbindung zwischen Funkbasisstation und der Hauptverbindungsstelle in Hall können die Funkgeräte im Sendebereich der Basisstation in einem topographieabhängigen Radius von

10 – 15 km weiterbetrieben werden („Local site trunking mode“). Gespräche über den Sendebereich der Basiszelle hinaus sind nicht möglich.

Die Basisstation signalisiert dabei den Endgeräten durch das Blinken einer gelben LED den geänderten Modus.

Main Switching Office – MSO

Die zentrale Verbindungsstelle in Hall verfügt über eine USV-Anlage und ein fest eingebautes Notstromaggregat. Dieses stellt die Stromversorgung für 7 Tage (ohne auftanken zu müssen) sicher.

Endgeräte

- **Fixstationen**

Die Fixstationen sind fest eingebaute Funkgeräte in Gebäuden. Diese werden über Netzstrom versorgt. Falls das Gebäude nicht notstromversorgt ist, müssen diese Geräte an eine externe Batterie angeschlossen werden.

- **Mobilfunkgeräte**

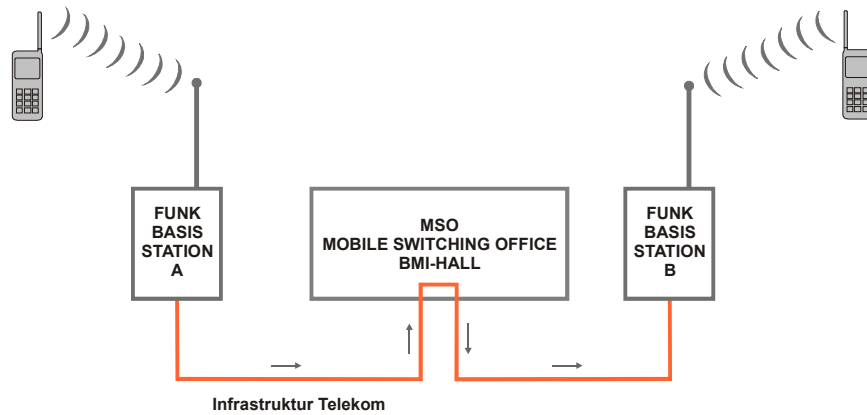
Diese Geräte sind in Fahrzeugen montiert und werden über die Fahrzeugbatterie versorgt.

Solange das Fahrzeug mit Treibstoff versorgt wird, ist die Stromversorgung der Geräte sichergestellt.

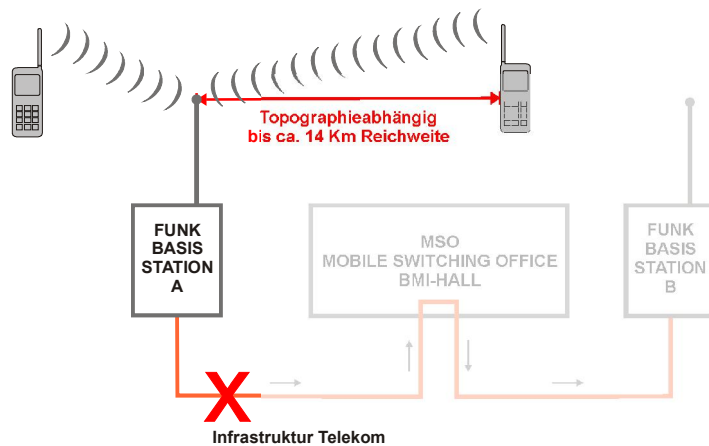
- **Handfunkgeräte**

Werden über Akkus versorgt. Aufgeladen stellen sie einen Betrieb von 14 Stunden sicher. Die Batterien können bei Stromausfall über Ladestationen an Fahrzeugen oder in notstromversorgten Gebäuden aufgeladen werden.

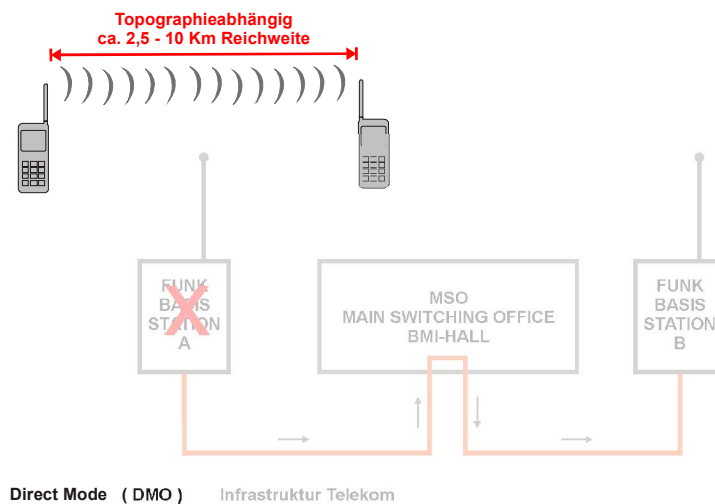
Die durchschnittliche Ladedauer eines leeren Akkus beträgt bis zu einer Stunde.



1. Normalbetrieb

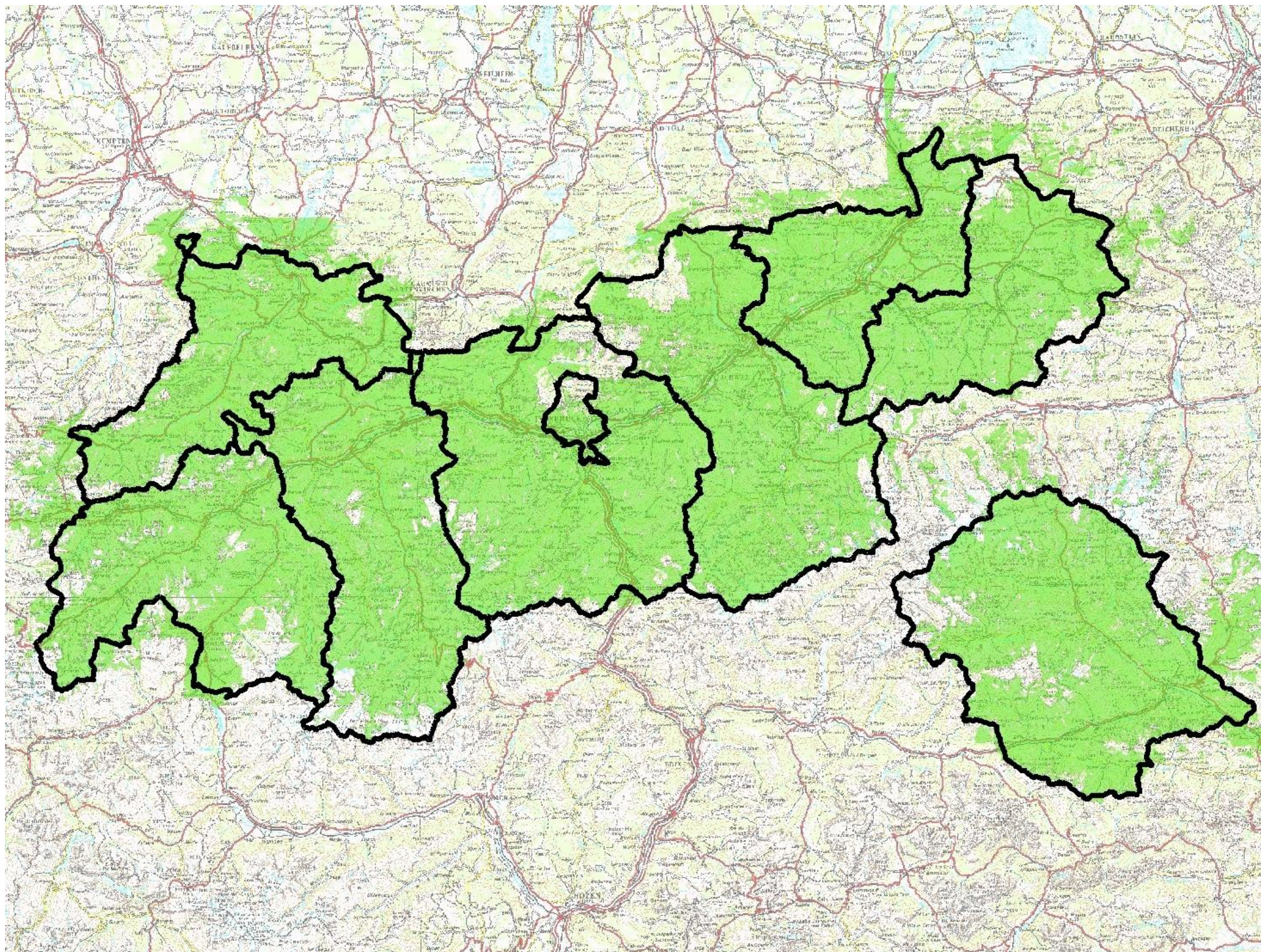


2. Betrieb bei Ausfall Verbindungsnetzwerk („Local site trunking mode“)



3. Betrieb bei Ausfall Basisstation (Direct Mode Operation – DMO)

1.2.4.12 Digitalfunk BOS Austria – Netzabdeckung Tirol



Grafik Digitalfunk BOS Austria – Netzabdeckung Tirol

(Quelle: Tiris, Stand 2008)

1.2.4.13 Warn- und Alarmierungssystem Tirol WAS – Tirol

Struktur

Zur Alarmierung von Einsatzkräften (BOS) und zur Warnung der Bevölkerung in Gefahrensituationen wird in Tirol das Warn- und Alarmierungssystem Tirol (WAS - Tirol) betrieben. Die Einsatzkräfte werden dabei über Pager und Sirenen verständigt. Die Bevölkerung wird über die Zivilschutzsignale der Sirenen gewarnt.

Die Alarmer können von der Landeswarnzentrale und der Leitstelle Tirol für das ganze Land, oder von den 8 Bezirkszentralen für den jeweiligen Bezirk ausgelöst werden. Über ein eigenes unabhängiges Sendernetz werden in ganz Tirol die Feuerwehr- und Zivilschutzsirenen sowie die Pager der Einsatzkräfte aktiviert.

Alle Systeme, Rechner, Datenbanken und Datenübertragungen sind redundant ausgeführt. An den 10 Auslösestandorten gibt es, neben doppelt ausgeführten PC-gestützten Arbeitsplätzen (zweiter PC ist Notbedienebene 1, NB1), eine weitere Rückfallebene. Mit Hilfe der Notbedienebene 2 kann die Alarmierung aller Einheiten ohne PC Unterstützung durchgeführt werden. Die Verteilung der Signale erfolgt über eigene Funkstrecken. Bei Ausfall dieser Funkanlagen wird die Alarmierung parallel über das Digitalfunknetz BOS Austria sichergestellt.

Verhalten des Warn- und Alarmsystems bei Stromausfall

Die PCs und die Notbedienebene NB1 in den Auslösestellen sind mit einer USV notstromversorgt. Die Autonomiezeit beträgt eine Stunde. Alle 10 Auslösestellen sind mit einer externen Einspeisestelle für die Stromversorgung über ein mobiles Notstromaggregat ausgestattet. Der Anschluss des Aggregates und die Umschaltung erfolgt durch geschultes Personal der Feuerwehr. Alle Senderstandorte sowie die Notbedienebene 2 (NB2) sind mit USV-Anlagen ausgestattet, die Überbrückungszeit beträgt 48 Stunden.

Sendeanlagen

Im Normalbetrieb werden die ausgelösten Alarme über die unabhängigen Sendeanlagen des WAS Tirol zu den Endgeräten übertragen, die jeweiligen Alarmumsetzer sind zusätzlich über das BOS Digitalfunknetz Tirol als „zweiten Weg“ angebunden. Bei Ausfall eines Systems werden die Alarmierungen automatisch über das andere geführt.

Die Sendeanlagen des WAS Tirol sind mit USV Anlagen für eine Betriebszeit von 48 Stunden ausgestattet. Auch diese Anlagen können mit mobilen Notstromaggregaten versorgt werden.

Alarmierungsendgeräte

Pager

Die Pager werden mit Batterien oder Akkus betrieben. Die Betriebsdauer der Pager beträgt damit bis zu zwei Monate.

Sirenen

1. Motorsirenen

Motorsirenen benötigen die Stromversorgung über das Netz. Ist keine Netzspannung verfügbar, funktionieren sie nicht.

2. Elektronische Sirene

Diese Sirene wird mittels Batterien betrieben, welche über einen Netzanschluss aufgeladen werden. Nach Ausfall der Netzstromversorgung bleiben die elektronischen Sirenen 7 Tage im Standby-Betrieb. In diesem Zeitraum sind mindestens 2 Alarmierungen sichergestellt. Vor Ausfall der Batterien meldet das Überwachungssystem diesen Zustand.

1.3.1 Standardführungsorganisation im Katastrophenfall

Außergewöhnliche Ereignisse, wie flächendeckende Strom- und IKT-Ausfälle, stellen eine konkrete Gefahr für die Versorgung der Bevölkerung mit lebenswichtigen Gütern und Dienstleistungen dar.

Dies macht im Sinne der Katastrophenschutzgesetzgebung eine koordinierte Führung durch die Behörde erforderlich. Im Falle einer Katastrophe wird durch das Katastrophenmanagementgesetz Tirol vorgeschrieben, wer als behördlicher Einsatzleiter (Bürgermeister, Bezirksverwaltungsbehörde, Landesregierung) tätig wird.

Behörden bilden dazu Führungsstäbe und verfügen über Einsatzorganisationen. Idealerweise bilden die „nicht behördlichen“ Partner im Zivil- und Katastrophenschutz auch Führungsstäbe, mit denen sie im Katastrophenfall ihre internen Strukturen leiten und mit externen Partnern und Strukturen kommunizieren.

Mit der Veröffentlichung der „Richtlinien für das Führen im Katastropheneinsatz“ durch das Staatliche Krisen- und Katastrophenmanagement soll eine „Vereinheitlichung im Bereich des Führens“ zur Gewährleistung der Interoperabilität zwischen Behörden, Einrichtungen und Einsatzorganisationen im Katastrophenfall erreicht werden.

Zur Erreichung dieser Ziele bedarf es eines einheitlichen Führungssystems.

Dieses besteht in Österreich aus:

- Führungsorganisation
- Führungsverfahren
- Führungsmittel

1.3.1.1 Führungsorganisation

Die Führungsorganisation besteht aus:

- vertikal aus einer auf mehreren Ebenen gegliederten Führungshierarchie
- der Zuordnung von Kompetenzen und Aufgaben an einzelne Elemente innerhalb der Hierarchie
- der Regelung der Abläufe innerhalb und zwischen den Elementen
- einer Regelung der Schnittstellen nach außen
- der klaren Rollenzuteilung für die einzelnen Elemente als Vorgesetzte oder Nachgeordnete

Als Beispiel ist die Führungsorganisation des Landes Tirol unter Punkt 1.3.2 dargestellt.

Die gegenseitige Vernetzung der Führungsorganisationen von Behörden und anderen Partnern im Zivil- und Katastrophenschutz ist für eine erfolgreiche Bewältigung von Notlagen unerlässlich.

1.3.1.2 Führungsverfahren

Das Führungsverfahren ist ein zielgerichteter, in sich geschlossener Ablauf, in dem

- Handlungsanweisungen für Nachgeordnete in der Führungsstruktur zur Durchführung des gestellten Auftrages erstellt werden
- Handlungsanweisungen an Nachgeordnete innerhalb der Hierarchie übermittelt werden
- die Umsetzung der Handlungsanweisungen kontrolliert wird

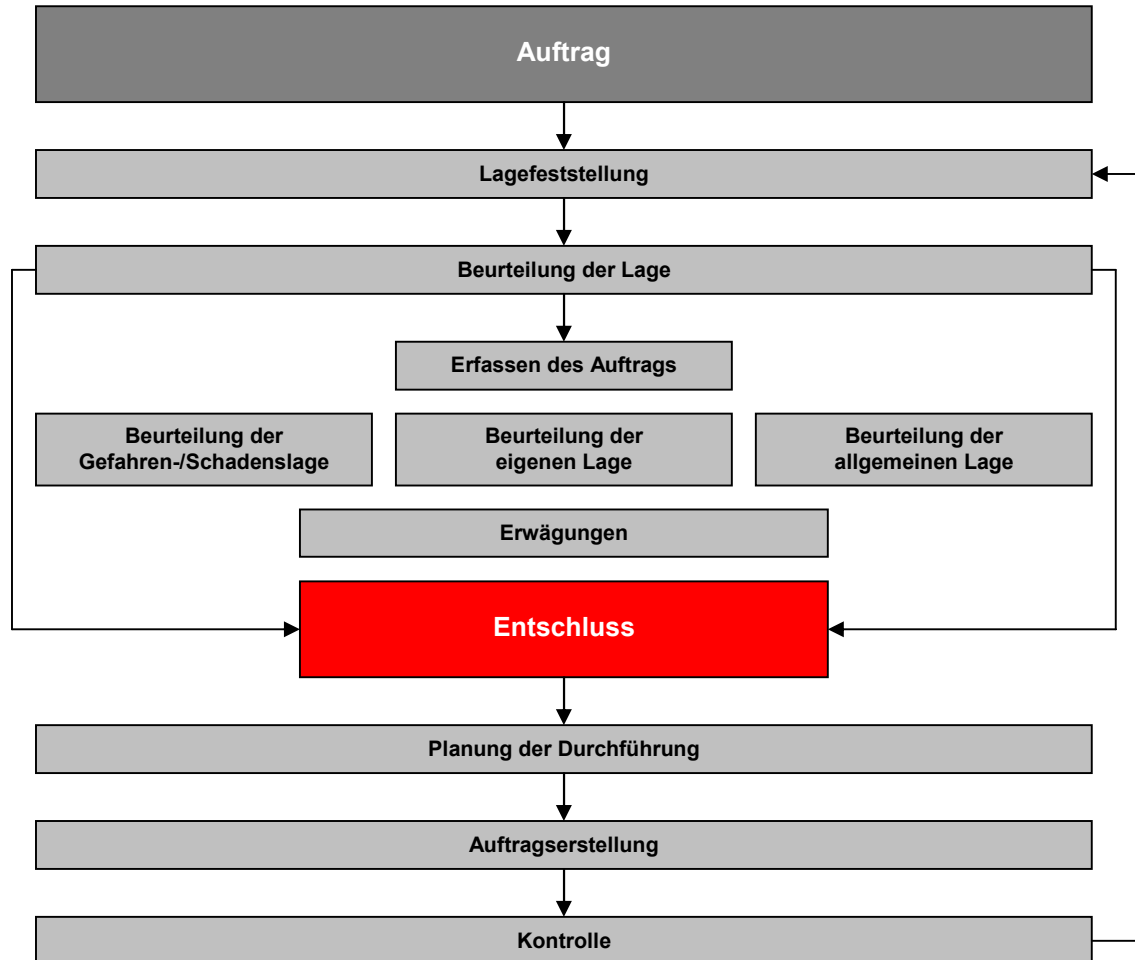
Regelkreis der Führung

Der Regelkreis der Führung wird durch einen anlassbezogenen Auftrag ausgelöst. Zuerst muss die Lage festgestellt werden. Nur auf der Basis von genauem und vor allem aktuellem Wissen der Lage kann diese richtig beurteilt werden. Die Lagebeurteilung ist die Grundlage für die Erwägung von Maßnahmen, die mit dem Entschluss entschieden werden.

Der Entschluss wird in Handlungsanweisungen (Befehl) für die Nachgeordneten umgesetzt und an alle Zuständigen in Form einer Auftragserteilung übermittelt.

Der nächste Schritt ist die Überwachung der Aufträge (Kontrolle).

Mit der neuerlichen Lagefeststellung beginnt der Regelkreis wieder von vorne und dauert so lange an, bis die Notlage beendet ist.



Grafik Regelkreis der Führung

(Quelle: Richtlinie für das Führen im Zivil- und Katastrophenschutz)

1.3.1.3 Führungsmittel

Als Führungsmittel wird das gesamte erforderliche Instrumentarium zum Gewinnen, Erfassen, Darstellen, Verarbeiten und Übermitteln von Informationen bezeichnet.

Führungsmittel reichen von Schreibgerät, Wandtafeln zur Lagedarstellung, Datensammlungen, Nachschlagewerken, Kartenmaterial bis zu Nachrichtenmitteln und Kommunikationssystemen, z.B. ESIS Tirol (digitales internetgebundenes Einsatzinformationssystem).

Der Begriff „Information“ ist dabei im weitesten Sinne zu verstehen – unabhängig von der Darstellungsform.

Darstellungsformen von Information sind unter anderem: direkte mündliche Mitteilung, Funkspruch, Telefonat, E-Mail, Meldung, Auftrag, Befehl, Lagevortrag, Notruf, Informationen in digitaler und analoger Form auf Bildschirmen, Projektoren, aus Karten und Planmaterial, Notfallpläne, Lagekarte, Checklisten usw.

Damit Führungsmittel erfolgreich eingesetzt werden können, werden auch Strukturen wie Gebäude, Sitzungsräume und Leitstellen benötigt.

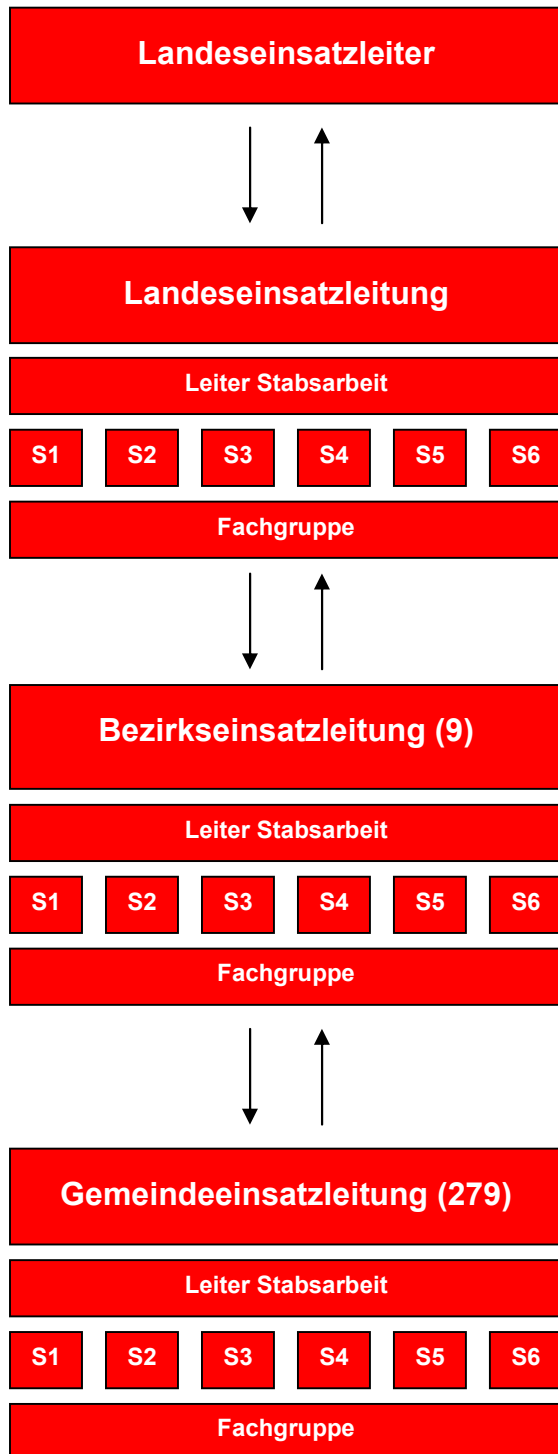
Zur Gewinnung von Information im Einsatzfall ist auch die Funktion von strategisch wichtigen innerbetrieblichen Strukturen und deren Ausfallsicherheit erforderlich.

Ohne Führungsmittel ist keine Führung möglich! Daher muss für Ausfallsicherheit gesorgt sein.

1.3.2 Katastrophen-Führungsorganisation in Tirol

1.3.2.1 Führung und Kommunikation der Partner im Zivil- und Katastrophenschutz

Die Partner gehören mit anderen Fachberatern der Fachgruppe an.

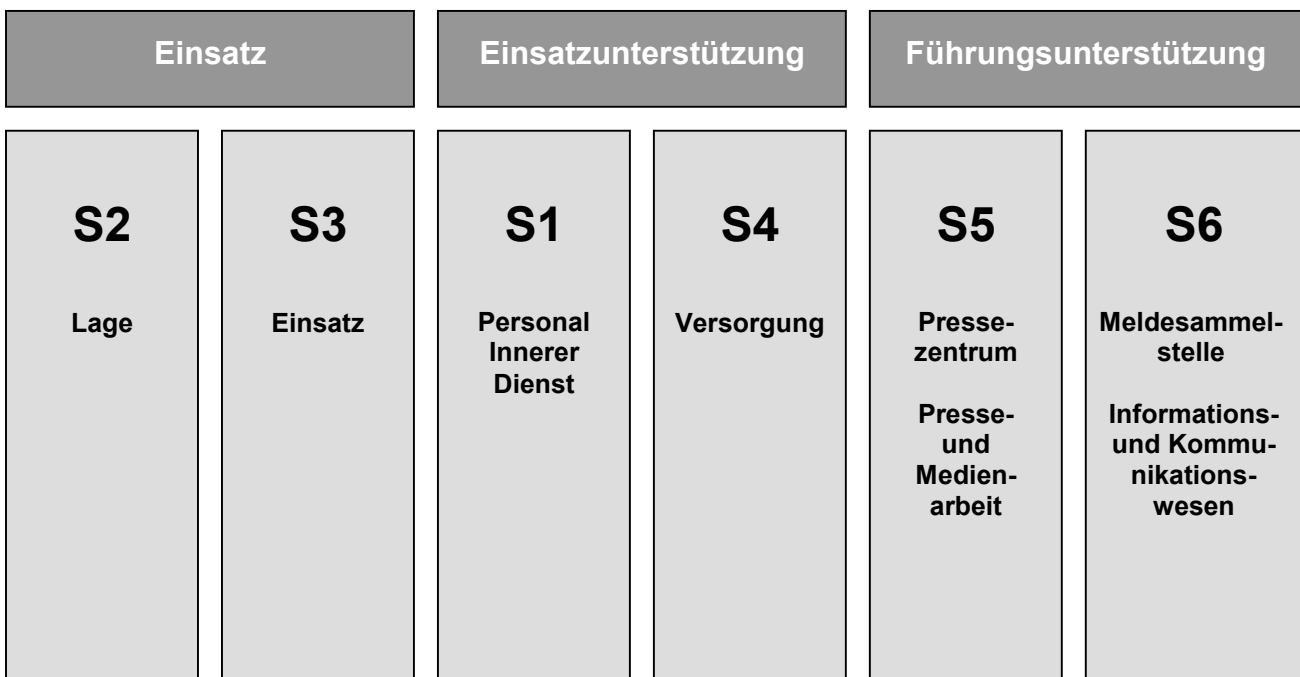


1.3.2.2 Führungsstab

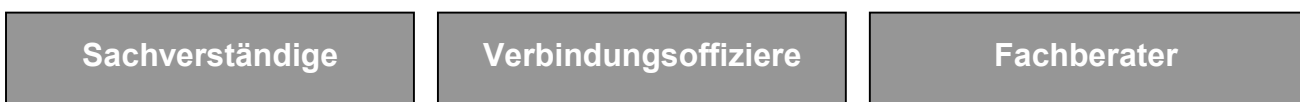
Zur Entlastung des Einsatzleiters und zur Bewältigung umfangreicher Führungsaufgaben wird ein Stab eingesetzt. Der Stab wird geführt vom Leiter Stabsarbeit. Die zu bewältigenden Aufgaben werden in Sachgebiete S1 bis S6 eingeteilt. Zum Stab dazugeholt werden je nach Bedarf Sachverständige, Verbindungsoffiziere und Fachberater.

Leiter Stabsarbeit

Führungsgruppe



Fachgruppe



Grafik Führungsstab

1.3.2.3 Aufgaben Leiter Stabsarbeit und Sachgebiete S1 – S6

Die Aufgabenverteilung innerhalb des Stabes kann aus der folgenden Grafik entnommen werden. Präzisiert werden muss, dass der Einsatzleiter nicht unmittelbar dem Stab angehört. Er bewegt sich auch außerhalb des Stabsraumes – gegenseitige Erreichbarkeit muss immer gewährleistet sein.

Einsatzleiter	<ul style="list-style-type: none"> Führen des Einsatzes
Leiter Stabsarbeit	<ul style="list-style-type: none"> Vertreten des Einsatzleiters Betreuen der Schnittstelle zu Einsatzleiter und anderen Organisieren der Stabsarbeit
S1	<ul style="list-style-type: none"> Erfassen und Organisieren der Einsatzkräfte Organisieren des Personals für die Stabsarbeit
S2	<ul style="list-style-type: none"> Lagefeststellung Lagedarstellung Beurteilung der Lage Lageinformation
S3	<ul style="list-style-type: none"> Vertreten des Leiter der Stabsarbeit Einsatzplanung und Einsatzdurchführung Dokumentieren des Einsatzablaufes
S4	<ul style="list-style-type: none"> Versorgung Organisieren von Fremdleistungen Verwaltung und Verrechnung Ganzheitliche Betreuung
S5	<ul style="list-style-type: none"> Medienarbeit Betreuung der Besucher Bilddokumentation Auskunft
S6	<ul style="list-style-type: none"> Ausstattung des Stabes Kommunikationsorganisation Einsatzdokumentation

Grafik Aufgaben Einsatzleiter und Führungsstab

(Quelle: Richtlinie für das Führen im Zivil- und Katastrophenschutz)

2.1 Stromversorgung

Mit Hilfe der folgenden Checklisten können die Partner im Zivil- und Katastrophenschutz schnell und strukturiert ermitteln, ob zur Aufrechterhaltung der Führung bei Netzstromausfall

- eine Notstromversorgung benötigt wird
- welche Einrichtungen, Anlagen und Geräte notstromversorgt werden müssen (= Ermittlung des Grundbedarfs)
- welche Art von Notstromversorgung erforderlich ist
- Ausrichtung der Berechnungen auf die eigene ungünstigste Situation

Checkliste nach Tätigkeiten

Was muss bei Stromausfall in Betrieb bleiben?

1	Gebäude / Strukturen	2.1.1
2	Kommunikation	2.1.2
3	Datenverarbeitung	2.1.3

	Checklisten zur Einsatzvorbereitung: Stromversorgung	2.1
--	---	------------

Gebäude/Strukturen	2.1.1
---------------------------	--------------

Welche Anlage/Geräte/Einrichtungen werden für die Führung im Einsatzfall benötigt?

<input type="checkbox"/>	ja	Elektrische Tore bzw. Türen, Schranken	nein	
↓	↓		↓	↓
<input type="checkbox"/>	ja	Zutrittssysteme	nein	
↓	↓		↓	↓
<input type="checkbox"/>	ja	Aufzüge	nein	
↓	↓		↓	↓
<input type="checkbox"/>	ja	Beleuchtung/Notbeleuchtung	nein	
↓	↓		↓	↓
<input type="checkbox"/>	ja	Heizung	nein	
↓	↓		↓	↓
<input type="checkbox"/>	ja	Lüftung / Klima	nein	
↓	↓		↓	↓
<input type="checkbox"/>	ja	Wasserversorgung	nein	
↓	↓		↓	↓
<input type="checkbox"/>	ja	Entsorgung	nein	
↓	↓		↓	↓
<input type="checkbox"/>	ja	Kopierer	nein	
↓	↓		↓	↓
<input type="checkbox"/>	ja	Brandmeldeanlagen	nein	
↓	↓		↓	↓
<input type="checkbox"/>	ja	Überwachungsanlagen	nein	
↓	↓		↓	↓
<input type="checkbox"/>	ja	Rundfunk- und Fernsehgeräte	nein	
↓	↓		↓	↓
<input type="checkbox"/>	ja	Kochgelegenheit	nein	
↓	↓		↓	↓
<input type="checkbox"/>	ja	Kaffeemaschine	nein	
↓	↓		↓	↓
<input type="checkbox"/>				
↓	↓		↓	↓
<input type="checkbox"/>				

**Bei einem oder mehreren angekreuzten Kästchen in der Spalte:
Notstromversorgung erforderlich**

Keine Notstromversorgung für angekreuzte Anlagen/Geräte/Einrichtungen erforderlich

Checkliste 2.1.4

	Checklisten zur Einsatzvorbereitung: Stromversorgung	2.1
--	---	------------

Kommunikation	2.1.2
----------------------	--------------

Welche Kommunikationsmittel sind für die Führung im Einsatzfall erforderlich?			
--	--	--	--

<input type="checkbox"/>		Analoges Telefon ¹	ja	
<input type="checkbox"/>		Digitales Telefon – Erstgerät an ISDN-Basisanschluss ²	ja	
<input checked="" type="checkbox"/>	ja	Digitales Telefon – weitere Geräte an ISDN-Basisanschluss ³	nein	
<input checked="" type="checkbox"/>	ja	Digitales Telefon – Geräte an ISDN-Multi- od. Primaryanschluss ⁴	nein	
<input checked="" type="checkbox"/>	ja	Mobiltelefon mit Netz-Aufladegerät	nein	
<input type="checkbox"/>		Mobiltelefon nur mit Pkw-Aufladegerät	ja	
<input checked="" type="checkbox"/>	ja	Fax	nein	
<input checked="" type="checkbox"/>	ja	PC – E-Mail	nein	
<input checked="" type="checkbox"/>	ja	Funk-Fixstation	nein	
<input checked="" type="checkbox"/>	ja	Mobilfunk mit Netz-Aufladegerät	nein	
<input type="checkbox"/>		Mobilfunk nur mit Pkw-Aufladegerät	ja	
<input checked="" type="checkbox"/>	ja	Satellitentelefon mit Netz-Aufladegerät	nein	
<input type="checkbox"/>		Satellitentelefon nur mit Pkw-Aufladegerät	ja	
<input type="checkbox"/>				

**Bei einem oder mehreren angekreuzten
Kästchen in der Spalte:
Notstromversorgung erforderlich**

**Notstromversorgung
für angekreuzte
Kommunikationsmittel nicht
erforderlich**

Checkliste 2.1.4

¹ Analoge Telefone (POTS) benötigen keine lokale Stromversorgung
² Ein digitales Telefon an ISDN-Basisanschluss benötigt bei richtiger Installation keine lokale Stromversorgung
³ Weitere digitale Telefongeräte an ISDN-Basisanschluss benötigen die lokale Stromversorgung
⁴ Telefongeräte an Multi- oder Primaryanschluss benötigen immer die lokale Stromversorgung

	Checklisten zur Einsatzvorbereitung: Stromversorgung	2.1
--	---	------------

Datenverarbeitung	2.1.3
--------------------------	--------------

Welche Datenverarbeitungsgeräte sind für die Führung im Einsatzfall erforderlich?

<input type="checkbox"/>	ja	Server	nein	
<input type="checkbox"/>	ja	Netzwerkssysteme	nein	
<input type="checkbox"/>	ja	Arbeitsplatzsysteme (PC, Tastatur, Bildschirm)	nein	
<input type="checkbox"/>	ja	Ein- und Ausgabegeräte (Scanner, Drucker, Plotter, Projektor)	nein	
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				

**Bei einem oder mehreren angekreuzten Kästchen in der Spalte:
Notstromversorgung erforderlich**

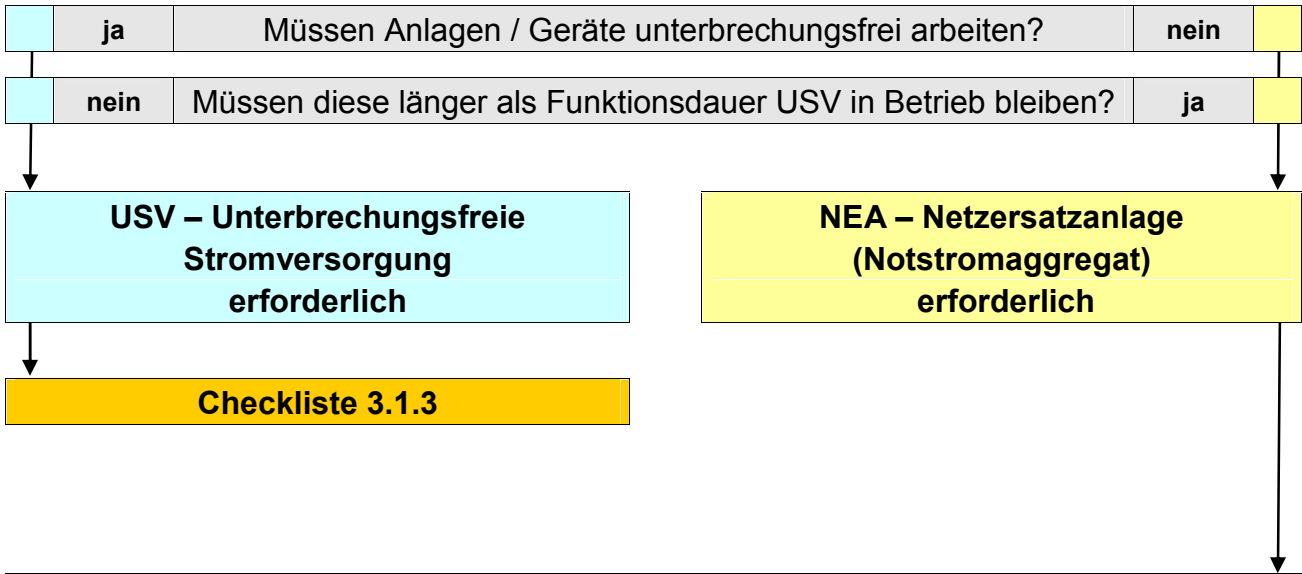
Keine Notstromversorgung für angekreuzte Datenverarbeitungsgeräte erforderlich

Checkliste 2.1.4

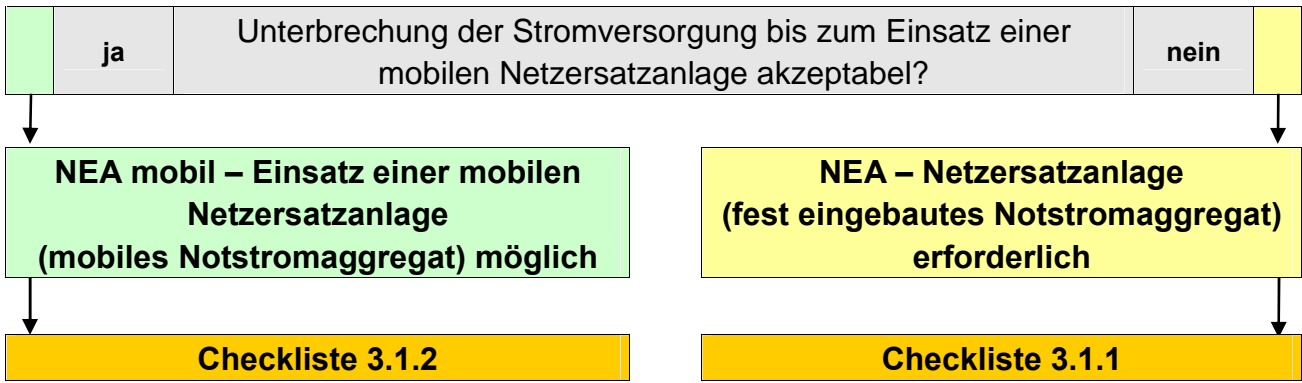
	Checklisten zur Einsatzvorbereitung: Stromversorgung	2.1
--	---	------------

Notstromversorgung ist erforderlich	2.1.4
--	--------------

Auswahl der Notstromversorgung



Auswahl der Netzersatzanlage



2.2 IKT-Versorgung

Mit Hilfe der folgenden Checklisten können die Partner im Zivil- und Katastrophenschutz schnell und strukturiert ermitteln, ob zur Aufrechterhaltung der Führung bei IKT-Ausfall

- eine IKT-Versorgung benötigt wird
- welche KT-Einrichtungen (Kommunikationsmittel) benötigt werden
- welche IT-Einrichtungen (Datenverarbeitung) benötigt werden
- welche Schutzmaßnahmen für die einzelnen Einrichtungen zu treffen sind

Checkliste nach Tätigkeiten

Was muss bei IKT-Ausfall in Betrieb bleiben?

1	Kommunikationstechnologie	2.2.1
2	Informationstechnologie – physikalische Leitungen	2.2.2
3	Informationstechnologie – Geräte/Systeme	2.2.3

Kommunikationstechnologie

2.2.1

Welche Technologie ist für die Führung im Einsatzfall erforderlich?

ja	Analoger Anschluss: analoge Telefone (POTS), Internet, E-Mail	nein	
ja	ISDN-Basisanschluss: analoge Telefone (POTS), digitale Telefone, Internet, E-Mail	nein	
ja	ISDN-Multi-/Primaryanschluss: HDSL, digitale Telefone, Internet, E-Mail	nein	
ja	Breitbandanschluss: XDSL (ADSL, VDSL, SDSL), Internet, E-Mail, VOIP	nein	
ja	UMTS-Mobiltelefonie	nein	
ja	EDGE-Mobiltelefonie	nein	
ja	GPRS-Mobiltelefonie	nein	
ja	Funk – analog	nein	
ja	Funk – digital	nein	
ja	Satellitentelefon	nein	
ja	Internet via WLAN	nein	

Sind Grundschutzmaßnahmen IKT getroffen?

ja nein

Grundschutzmaßnahmen treffen

Checkliste 3.2.1

Steht eine redundante oder Ersatz-Technologie zur Verfügung?

ja nein

Redundanz bzw. Ersatzmaßnahmen treffen

Checkliste 3.2.2

Notmaßnahmen für IKT-Komplettausfall treffen

Checkliste 3.2.6

Keine Maßnahmen für angekreuzte Technologien erforderlich

Informationstechnologie – physikalische Leitungen

2.2.2

Über welche physikalische Leitung geht Ihre externe IT-Anbindung?

<input type="checkbox"/>	ja	Physikalisch eigenständige Standleitung	nein	<input type="checkbox"/>
<input type="checkbox"/>	ja	Telefonfestnetz	nein	<input type="checkbox"/>
<input type="checkbox"/>	ja	TV-Kabel	nein	<input type="checkbox"/>
<input type="checkbox"/>	ja	Funkanbindung – WLAN	nein	<input type="checkbox"/>
<input type="checkbox"/>	ja	Mobiltelefonie (UMTS, EDGE, GPRS)	nein	<input type="checkbox"/>
<input type="checkbox"/>	ja	Satellitenanbindung – nur Download	nein	<input type="checkbox"/>
<input type="checkbox"/>	ja	Satellitenanbindung – Up- und Download	nein	<input type="checkbox"/>
<input type="checkbox"/>				<input type="checkbox"/>
<input type="checkbox"/>				<input type="checkbox"/>

Sind Grundschutzmaßnahmen IKT getroffen?

ja nein

Grundschutzmaßnahmen treffen

Checkliste 3.2.1

Steht eine redundante oder Ersatz-Technologie zur Verfügung?

ja nein

Redundanz bzw. Ersatzmaßnahmen treffen

Checkliste 3.2.3

Notmaßnahmen für IKT-Komplettausfall treffen

Checkliste 3.2.6

Keine Maßnahmen für angekreuzte Technologien erforderlich

Informationstechnologie – Geräte/Systeme

2.2.3

Welche Geräte / Systeme werden für die Führung im Einsatzfall benötigt?

ja	Server	nein	
ja	Netzwerkssystem – LAN	nein	
ja	Netzwerkssystem – WLAN	nein	
ja	Arbeitsplatzsysteme (PC, Tastatur, Bildschirm)	nein	
ja	Ein- und Ausgabegeräte (Scanner, Drucker, Plotter, Projektor)	nein	
ja	Notebook – LAN	nein	
ja	„Stand alone“-Geräte (ohne IT-Netzanbindung)	nein	
ja	Speichermedien	nein	

Sind Grundschutzmaßnahmen IKT getroffen?

ja nein

Grundschutzmaßnahmen treffen

Checkliste 3.2.1

Stehen redundante Technologien zur Verfügung?

ja nein

Redundanz bzw. Ersatzmaßnahmen treffen

Checkliste 3.2.4

Notmaßnahmen für IKT-Komplettausfall treffen

Checkliste 3.2.6

Keine Maßnahmen für angekreuzte Technologien erforderlich

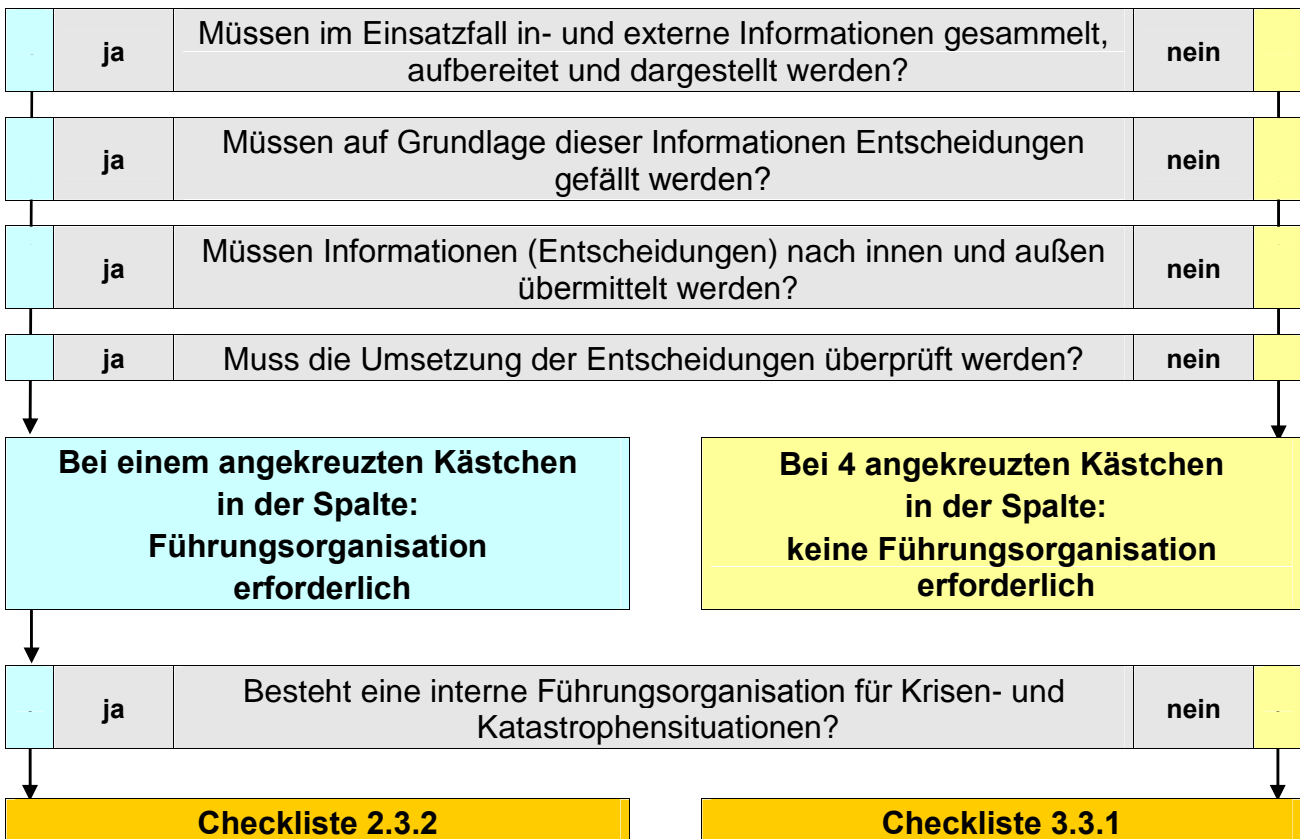
2.3 Führungsorganisation

Mit Hilfe der folgenden Checklisten können die Partner im Zivil- und Katastrophenschutz schnell und strukturiert ermitteln, ob zur Aufrechterhaltung der Führung bei Netzstrom- und IKT-Ausfall

- eine Führungsorganisation benötigt wird
- welche Führungsverfahren einen zielgerechten, geschlossenen Ablauf garantieren
- welche Führungsmittel erforderlich sind

Führungsorganisation – Ermittlung der Notwendigkeit	2.3.1
--	--------------

Wird eine Führungsorganisation im Einsatzfall benötigt?			
--	--	--	--



	Checklisten zur Einsatzvorbereitung: Führungsorganisation	2.3
--	--	------------

Führungsorganisation – Zuweisung der Sachgebiete	2.3.2
---	--------------

Sind folgende Sachgebiete in Ihrer Führungsorganisation klar definiert und an Personen zugewiesen?

<input type="checkbox"/>	ja	Fällen von Entscheidungen	nein	
↓				
<input type="checkbox"/>	ja	Hochfahren des Führungsstabes	nein	
↓				
<input type="checkbox"/>	ja	Personalmanagement	nein	
↓				
<input type="checkbox"/>	ja	Sammeln, Darstellen und Beurteilen von Informationen	nein	
↓				
<input type="checkbox"/>	ja	Planung und Durchführung von Maßnahmen Vorbereitung von Entscheidungen	nein	
↓				
<input type="checkbox"/>	ja	Dokumentation der Führungsarbeit	nein	
↓				
<input type="checkbox"/>	ja	Versorgung mit Material und Mitteln	nein	
↓				
<input type="checkbox"/>	ja	Organisation von Fremdleistungen	nein	
↓				
<input type="checkbox"/>	ja	Medienarbeit	nein	
↓				
<input type="checkbox"/>	ja	Technische Organisation und Betreuung der in- und externen Kommunikation	nein	

**Bei mehr als 7 angekreuzten Kästchen in der Spalte:
Die Sachgebiete in der Führungsstruktur sind strukturiert.
Eine mögliche Angleichung an die „Richtlinie für das Führen im Katastropheneinsatz“ – Aufbau einer Führungsorganisation – ist zu überprüfen**

Checkliste 3.3.1

**Rotes Kästchen oder mehr als 4 Kästchen in der Spalte angekreuzt:
Strukturierung der Sachgebiete erforderlich**

Checkliste 3.3.1

	Checklisten zur Einsatzvorbereitung: Führungsorganisation	2.3
--	--	------------

Führungsorganisation – Verankerung	2.3.3
---	--------------

<input type="checkbox"/>	ja	Werden innerhalb Ihrer Führungsorganisation die Sachgebiete (siehe 2.3.2) von mehr als drei Personen betreut?	nein	
↓	↓	↓	↓	↓
<input type="checkbox"/>	ja	Gibt es im Einsatzfall regelmäßige Besprechungen zwischen diesen Personen in einem Raum an einem Ort?	nein	
↓	↓	↓	↓	↓
<input type="checkbox"/>	ja	Werden die Mitglieder Ihrer Führungsorganisation regelmäßig geschult?	nein	
↓	↓	↓	↓	↓
<input type="checkbox"/>	ja	Gibt es Regeln zur Verhinderung von Informationsüberlastung einzelner Personen?	nein	
↓	↓	↓	↓	↓
<input type="checkbox"/>	ja	Gibt es im Einsatzfall ein Personalmanagement für den Führungsstab mit Dienstzeiten- und Versorgungsregelungen?	nein	
↓	↓	↓	↓	↓
<input type="checkbox"/>	ja	Berücksichtigen die Personal-, Dienstzeiten- und Versorgungsregelungen auch lang andauernde Einsätze über mehrere Tage und Wochen?	nein	
↓	↓	↓	↓	↓
<input type="checkbox"/>	ja	Ist das Führungsverfahren mittels Regelkreisen in Ihrer Führungsorganisation geregelt? (siehe Kap. 1.3.1.2)	nein	

**Bei 7 angekreuzten Kästchen
in der Spalte:
keine Maßnahmen erforderlich**

**Bei 1 angekreuzten Kästchen
in der Spalte:
Eine Angleichung an die „Richtlinie
für das Führen
im Katastropheneinsatz“ –
Aufbau einer Führungsorganisation –
wird empfohlen**

Checkliste 3.3.1

	Checklisten zur Einsatzvorbereitung: Führungsorganisation	2.3
--	--	------------

Führungsmittel	2.3.4
-----------------------	--------------

Die für die Führung erforderlichen IKT-Mittel, deren Stromversorgung, sowie die elektrisch betriebenen Gebäudeeinrichtungen und -ausstattungen wurden bereits unter den Punkten

- 2.1.1 Stromversorgung Gebäude/Strukturen
- 2.1.2 Stromversorgung Kommunikation
- 2.1.3 Stromversorgung Datenverarbeitung
- 2.1.4 Stromversorgung Notstromversorgung
- 2.2.1 Kommunikationstechnologie – KT
- 2.2.2 und 2.2.3 Informationstechnologie – IT

behandelt:

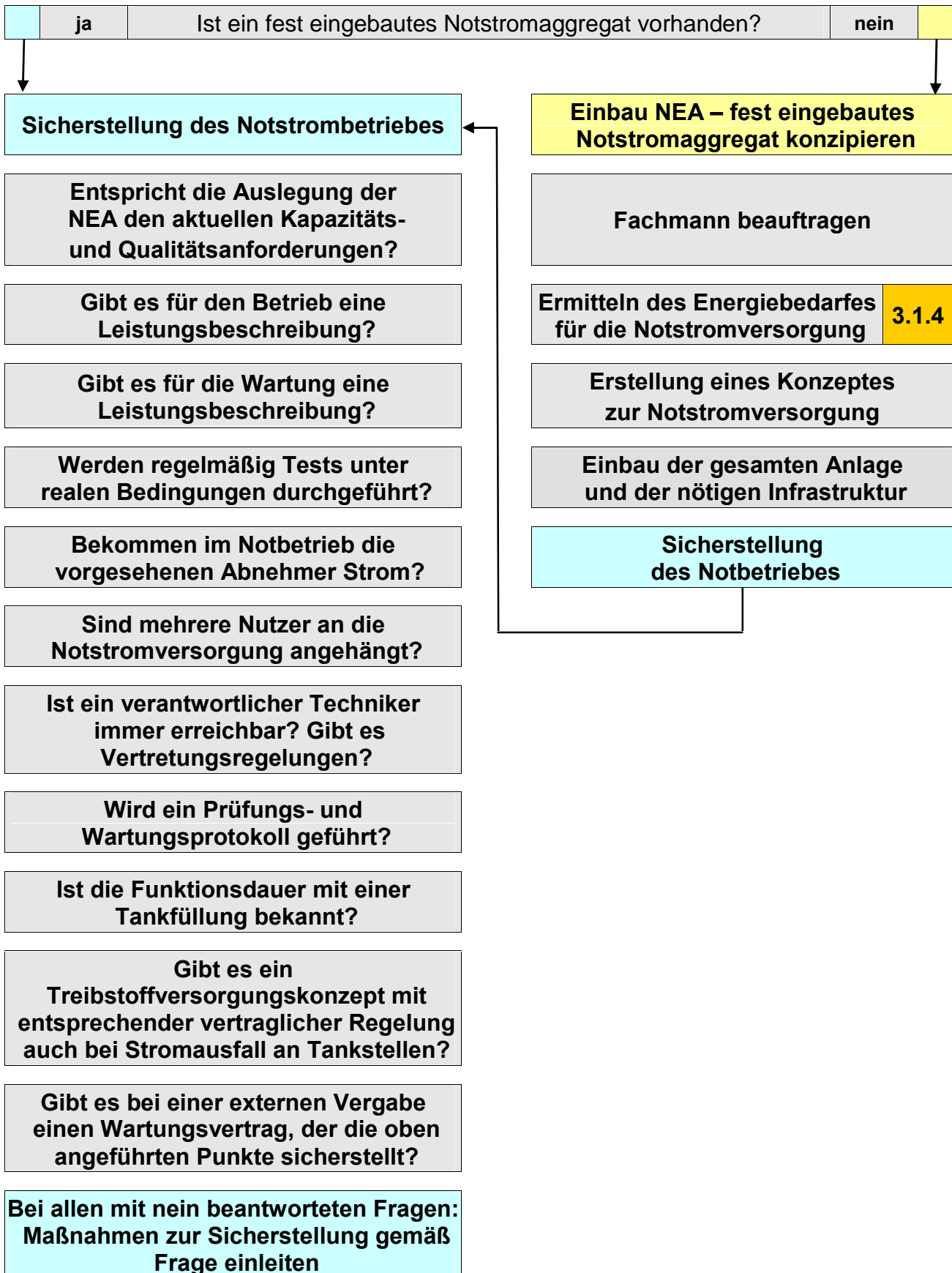
Sind die zusätzlich erforderlichen Führungsmittel vorhanden?			
---	--	--	--

<input type="checkbox"/>	ja	Sitzungsräume Führungsstab	nein	<input type="checkbox"/>
<input type="checkbox"/>	ja	Nachrichtenraum	nein	<input type="checkbox"/>
<input type="checkbox"/>	ja	Alarmierungspläne	nein	<input type="checkbox"/>
<input type="checkbox"/>	ja	Mitarbeiter-, Ressourcen-, Telefon- und Adressenlisten, Dienstpläne usw.	nein	<input type="checkbox"/>
<input type="checkbox"/>	ja	Checklisten für einzelne Stabsfunktionen	nein	<input type="checkbox"/>
<input type="checkbox"/>	ja	Material zur Lageführung und Darstellung	nein	<input type="checkbox"/>
<input type="checkbox"/>	ja	Kartenmaterial / Kartenwände	nein	<input type="checkbox"/>
<input type="checkbox"/>	ja	Meldeblöcke	nein	<input type="checkbox"/>
<input type="checkbox"/>	ja	Handlungsanweisungen (Checklisten)	nein	<input type="checkbox"/>
<input type="checkbox"/>	ja	Vordrucke zur Erstellung der Einsatzdokumentation	nein	<input type="checkbox"/>
<input type="checkbox"/>	ja	Vorlagen Pressearbeit	nein	<input type="checkbox"/>

**Alle mit nein angekreuzten Kästchen
in der Spalte:
entsprechende Führungsmittel sind
zu beschaffen bzw. einzurichten**

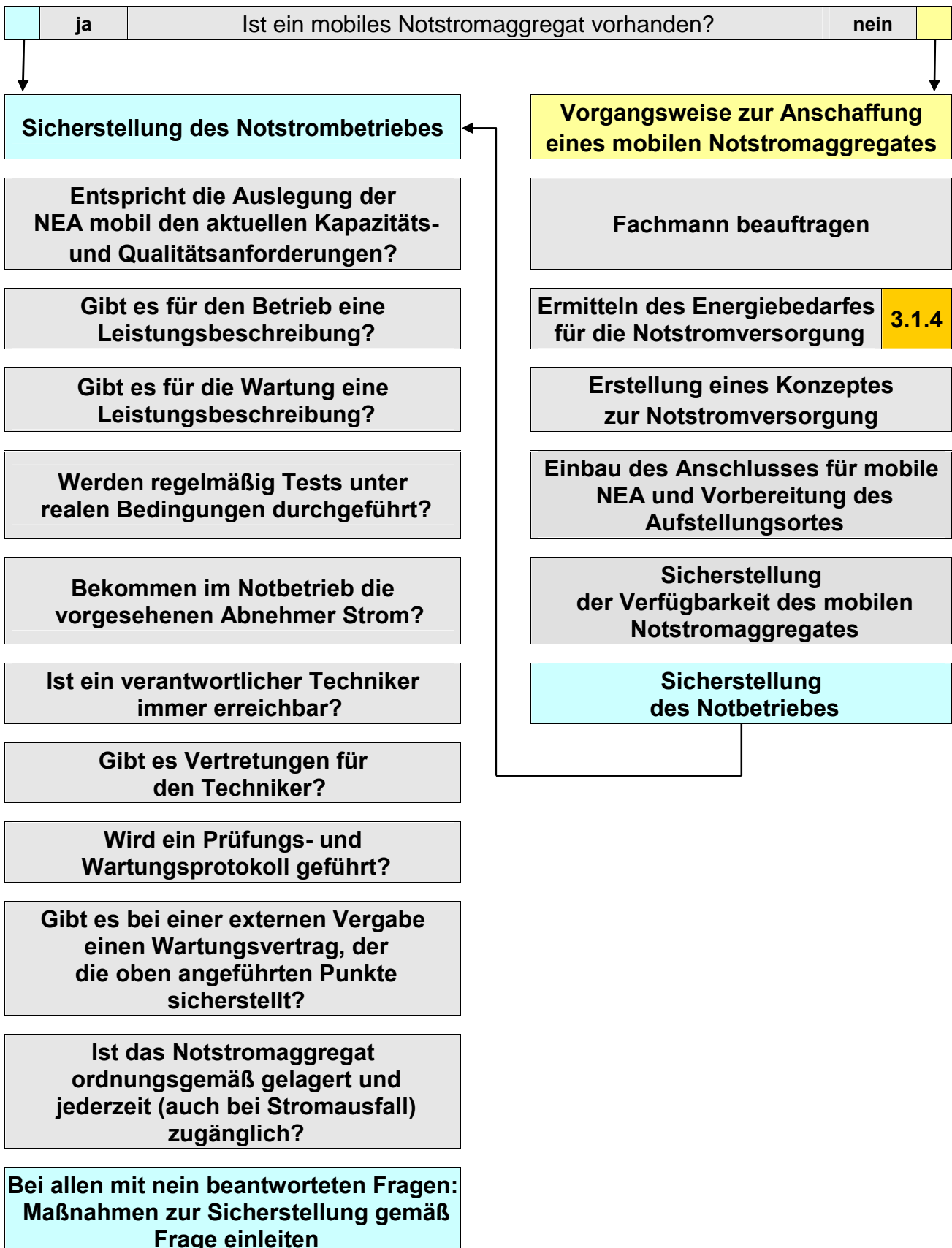
Netzersatzanlage (NEA) – fest eingebaut

3.1.1



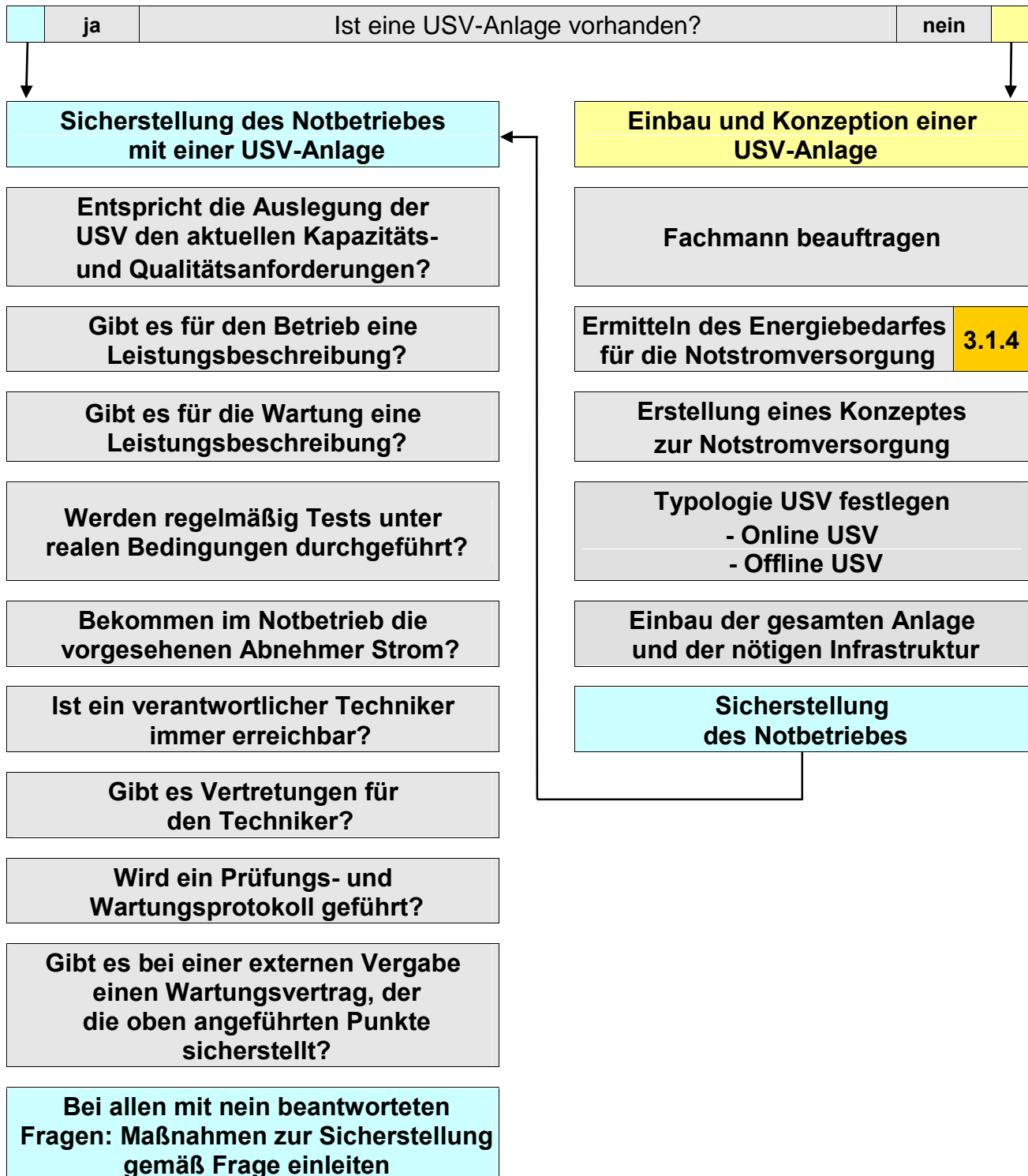
Netzersatzanlage (NEA) – mobil

3.1.2



Unterbrechungsfreie Stromversorgung – USV

3.1.3



Grundschutzmaßnahmen IKT**3.2.1**

Mit dem Begriff IT-Grundschutz werden Sicherheitsmaßnahmen bezeichnet, welche standardmäßig für IT-Systeme ergriffen werden sollten.

Dabei geht es um drei Grundwerte in der IT-Sicherheit:

1. **Vertraulichkeit**, Informationen müssen vor nicht autorisierter Weitergabe geschützt werden
2. **Verfügbarkeit**, das IT-System muss jederzeit die von ihm zu erbringenden Leistungen zur Verfügung stellen
3. **Integrität**, die Daten müssen immer vollständig und unverändert wiedergegeben werden

Ausführliche Unterlagen und Hilfen zum Aufbau eines IT-Grundschutzes können kostenlos von den Webseiten des A-SIT Zentrum für sichere Informationstechnologie Austria unter www.a-sit.at und dem deutschen Bundesamt für Sicherheit in der Informationstechnik unter www.bsi.bund.de/gshb eingesehen und heruntergeladen werden.

Im Anhang des Leitfadens IT-Sicherheit des deutschen Bundesamtes für Sicherheit in der Informationstechnik unter www.bsi.bund.de/gshb/Leitfaden/index.htm stehen 50 Fragen zur Verfügung, welche einen schnellen Überblick über die Schwachstellen in Ihrem Unternehmen ermöglichen. Dieser Check ist ein idealer Einstieg in die Materie. Er ist einfach gestaltet. Die Durchführung dieses Checks erfordert kein Expertenwissen.

Folgende Themen sind darin beinhaltet:

- IT-Sicherheitsmanagement
- Sicherheit von IT-Systemen
- Vernetzung und Internet-Anbindung
- Beachtung von Sicherheitserfordernissen
- Wartung von IT-Systemen / Umgang mit Updates
- Passwörter und Verschlüsselung
- Notfallvorsorge
- Datensicherung
- Infrastruktursicherheit

Ermittlung der Redundanzen bei Ausfall der Kommunikationstechnologie

3.2.2

	Analoger Anschluss	ISDN Basisanschluss	ISDN Multi-/Primaryanschluss	Breitbandanschluss	UMTS Mobiltelefonie	EDGE Mobiltelefonie	GPRS Mobiltelefonie	Funk analog	Funk digital	Satellitentelefon	WLAN
Analoger Anschluss											
ISDN Basisanschluss											
ISDN Multi-/Primaryanschluss											
Breitbandanschluss											
UMTS Mobiltelefonie											
EDGE Mobiltelefonie											
GPRS Mobiltelefonie											
Funk analog											
Funk digital											
Satellitentelefon											
WLAN											

● Redundanz: Leistung wird vollständig aufrechterhalten

■ Ersatz: Leistung wird teilweise ersetzt

▲ Notlösung: Leistung wird in geringem Umfang mit anderen Mitteln ersetzt

Redundanzen bei Ausfall IT – physikalische Leitungen

3.2.3

	Physikalisch eigenständige Leitung	Telefonfestnetz	TV-Kabel	Funkanbindung WLAN	Mobiltelefonie (UMTS, EDGE, GPRS)	Satellitenanbindung nur Download	Satellitenanbindung Up- und Download
Physikalisch eigenständige Leitung							
Telefonfestnetz							
TV-Kabel							
Funkanbindung WLAN							
Mobiltelefonie (UMTS, EDGE, GPRS)							
Satellitenanbindung nur Download							
Satellitenanbindung Up- und Download							

- Redundanz: Leistung wird vollständig aufrechterhalten
- Ersatz: Leistung wird teilweise ersetzt
- ▲ Notlösung: Leistung wird in geringem Umfang mit anderen Mitteln ersetzt

Redundanz bzw. Ersatz IT-Geräte/-Systeme**3.2.4**

Die erforderlichen IT-Geräte und -Systeme – um die Führung in Notsituationen aufrechtzuerhalten – wurden in der Checkliste 2.2.3 festgelegt.

Server

Server können durch gleichwertige redundante Systeme ersetzt werden. Ist dies nicht möglich, können von IT-Technikern mit geringem Aufwand Ersatzlösungen, wie unter 3.2.6 Informationstechnologie – IT beschrieben, eingerichtet werden.

Essenziell dabei ist, dass die Daten und Informationen, welche im Notfall wirklich gebraucht werden, über diese Ersatz- bzw. Notsysteme bereitgestellt werden.

Um den Zugriff für befugte Personen jederzeit sicherzustellen, müssen Passwörter und Zugriffscodes in Papierform an geschützter Stelle hinterlegt werden.

Netzwerke

Zur Aufrechterhaltung von Netzwerksystemen kann die Bereithaltung von „kritischen Elementen“, wie Switch und Router empfohlen werden.

Die „Ersatzteile“ sollten betriebsintern gelagert werden. Die Erreichbarkeit und der Einsatz von IT-Technikern ist jederzeit sicherzustellen.

Um den Zugriff für befugte Personen jederzeit sicherzustellen, müssen Passwörter und Zugriffscodes in Papierform an geschützter Stelle hinterlegt werden.

Arbeitsplatzsysteme / Ein- und Ausgabegeräte

Der Ersatz von Arbeitsplatzsystemen, Ein- und Ausgabegeräten sowie von Speichermedien ist normalerweise einfach. Da für die „Führung“ im Einsatzfall meist nicht alle vorhandenen Geräte gebraucht werden, können bei Ausfällen diese mit intern verfügbaren Geräten ersetzt werden. Dabei ist darauf zu achten, dass auch die entsprechenden Programme auf diesen Geräten vorhanden sind.

Der Einsatz von fachkundigem Personal ist sicherzustellen.

Ist ein interner Ersatz nicht möglich, wird der Abschluss von entsprechenden Serviceverträgen, mit den bereits für das Unternehmen bzw. die Behörde tätigen IT-Dienstleistern, empfohlen.

Um den Zugriff für befugte Personen jederzeit sicherzustellen, müssen Passwörter und Zugriffscodes in Papierform an geschützter Stelle hinterlegt werden.

Gleichwertige Telefonie- und IT-Dienstleistungen werden von mehreren Anbietern erbracht. Zur Aufrechterhaltung der Leistungen bei Ausfall eines Anbieters kann auf einen anderen zurückgegriffen werden. Dazu müssen rechtzeitig die Voraussetzungen geschaffen werden.

Kommunikationstechnologie – KT

Bei Ausfall des Festnetztelefonanbieters kann auf die Mobiltelefonie zurückgegriffen werden. Die Mobiltelefonnummern müssen umgehend oder bereits vorab bekanntgegeben werden. Web-Seiten sind dafür ein geeignetes Mittel. Die Veröffentlichung von Texten auf der eigenen Web-Seite sollte durch internes Personal durchführbar sein. Ist die Webseite über das Festnetz nicht erreichbar, kann dies über eine Mobiltelefonie-Steckkarte noch möglich sein. Diese ist bereitzuhalten.

Fällt ein Mobiltelefonanbieter aus, kann über das nationale Roaming auf einen anderen Anbieter gewechselt werden. Wie das möglich ist, wird unter Tipps und Tricks im Kapitel 3.4.1 beschrieben.

Informationstechnologie – IT

Für den Ausfall von Firmen- oder Behördennetzwerken sind eigene Vorkehrungen zu treffen. Dies kann in der Regel nur durch aufwändige redundante Systeme geschehen.

„Not-Web-Seiten“, welche zumindest die Information oder Dienste im geringen Ausmaß ermöglichen, können ohne großen Aufwand bei getrennten Anbietern bereitgehalten werden.

Keinen Aufwand verursachen „Reserve“ E-Mail Adressen. Diese können bei zahlreichen, freien, kostenlosen Anbietern eingerichtet werden. Damit die „Reserveadresse“ im Notfall allen Partnern bekannt gegeben werden kann, muss eine Mailingliste im digitalen Format, z. B. auf einem Word-Dokument bereitgehalten werden.

Damit „Notmaßnahmen“ schnell eingerichtet werden können, müssen genügend Personen bescheid wissen. Die zu treffenden Maßnahmen müssen geläufig sein. Dafür sind Schulungen und Übungen unter realen Bedingungen erforderlich.

Die Erreichbarkeit des zuständigen Personals oder externer Dienstleister muss jederzeit sichergestellt sein.

Kommunikationstechnologie – KT

Bei einem Komplettausfall aller Kommunikationsmittel kann eine behelfsmäßige Nachrichten-Übermittlung mittels Melder, das sind Personen, welche Nachrichten mündlich, schriftlich oder auf Datenträger persönlich überbringen, eingerichtet werden.

Vorab ist dafür die Erstellung eines Kommunikationsplanes mit folgendem Inhalt erforderlich:

- Definition der Stellen, mit denen im Einsatzfall unbedingt kommuniziert werden muss
- Festlegung von Hol- und Bringmeldungen
- Festlegung von Melde-Sammelpunkten, fixe Meldezeit-Intervalle
- Distanzen ermitteln und Einsatzbereitschaft der Fortbewegungsmittel garantieren
- Form der Kommunikation festlegen:
 - Mündliche Meldung – Nachricht wird mündlich überbracht
 - Schriftliche Meldung – Nachricht wird schriftlich überbracht
 - Fotos/Karten/Pläne – Nachricht wird auf Fotos, Karten und Plänen festgehalten und überbracht
 - Information auf Datenträger – Nachrichten werden auf Datenträgern gespeichert und diese werden überbracht
- Beschaffung aller Mittel, welche zur Erstellung der Mitteilungen benötigt werden
- Papier, Schreibzeug, Meldeblöcke mit mehreren Durchschlägen
- PC, Notebook, digitale Karten, Datenträger wie USB-Stick, CD-Rohlinge usw.

Informationstechnologie – IT

Die für die Führung im Einsatzfall erforderlichen digitalen Informationen sollten auf jeden Fall auf Datenträgern wie USB-Sticks, CD, DVD, auf „Stand alone“-PCs oder auf Notebooks bereitgehalten werden. Bei Komplettausfall der Stromversorgung und/oder von IKT-Systemen kann ein Notebook mit Stromanschlussvorrichtung für Fahrzeuge noch lange Zeit ohne herkömmliche Notstromversorgungssysteme betrieben werden.

Neben gespeichertem Wissen im Kopf von Menschen als allerletzte Rückfallebene stellen auf Papier gespeicherte Informationen immer noch die ausfallsicherste Variante dar.

Aus diesem Grund wird ausdrücklich empfohlen, unverzichtbare Informationen für den Einsatzfall in dieser Form an mindestens zwei verschiedenen Orten bereitzuhalten.

Zur Aufrechterhaltung von Minimalfunktionen bei einem IKT-Komplettausfall innerhalb der Strukturen der Partner im Zivil- und Katastrophenschutz können einfach gehaltene und den Mitarbeitern bekannte Formulare entscheidend beitragen.

Aufbau einer Führungsorganisation**3.3.1**

Der Aufbau von einheitlichen Führungsorganisationen bei den Partnern im Zivil- und Katastrophenschutz in Tirol ist ein zentrales Anliegen dieses Handbuches.

Im Einsatzfall wird das Zusammenspiel aller Partner über die jeweilige Führungsorganisation entscheidend für den gemeinsamen Einsatzerfolg sein.

In ganz Österreich wird zur Vereinheitlichung der Führungsorganisation im Katastrophenfall die Umsetzung der Richtlinien des Staatlichen Krisen- und Katastrophenmanagements (SKKM) empfohlen. Die Grundzüge der Richtlinie sind im Kapitel „1.3 Grundlagen Führungsorganisation“ dargestellt.

Die vollinhaltliche Richtlinie kann bei der Landeswarnzentrale Tirol (LWZ) angefordert werden.

Die Erfahrung der Autoren dieses Handbuches ist, dass die Richtlinien für das Führen im Katastropheneinsatz des SKKM gut an bestehende betriebliche Führungsstrukturen „angelegt“ werden kann.

Je nach Ergebnissen aus den Checklisten zur Einsatzvorbereitung können folgende Aufgabenstellungen anstehen:

- Aufbau der Führungsorganisation nach Richtlinien für das Führen im Katastropheneinsatz des SKKM
- Anpassung der Führungsorganisation an die Richtlinien für das Führen im Katastropheneinsatz des SKKM
- Strukturierung der Sachgebiete gemäß Richtlinien für das Führen im Katastropheneinsatz des SKKM

Unabhängig der zu treffenden Maßnahmen empfehlen wir die folgende Vorgangsweise:

1. Herbeiführung einer Entscheidung des innerhalb der eigenen Organisation zuständigen Organs oder Gremiums, die Richtlinien für das Führen im Katastropheneinsatz des SKKM zur Anwendung zu bringen.
2. Aufbau der Führungsorganisation bzw. deren Anpassung an die Richtlinien für das Führen im Katastropheneinsatz des SKKM.
3. Klare Zuweisung der Funktionen der Verantwortung und der Kompetenzen im Einsatzfall an Personen.
4. Darstellung der möglichen Maßnahmen des Krisenmanagements im Einsatzfall realistisch ansetzen, um die üblicherweise sehr hohe Erwartungshaltung an das Krisenmanagement zurechtzurücken.
5. Die Implementierung gründlich durchführen:
Dabei muss sichergestellt werden, dass alle Beteiligten (interne und externe) über die neue Führungsorganisation genauestens informiert werden und über ihre Rolle und Aufgaben Bescheid wissen.
6. Regelmäßig schulen und üben, üben, üben. Ernstfälle treten glücklicherweise selten ein. Deshalb sind Praxiserfahrungen auch rar. Trotzdem muss die Führungsorganisation im Ernstfall perfekt funktionieren und die erwarteten Leistungen bringen. Mangelnde Praxiserfahrung kann durch ausreichende Schulung und mit regelmäßigen, praxisnahen Übungen, Workshops und Einsatzsimulationen ausgeglichen werden.

In diesem Teil findet der Leser Tipps und Tricks von den Partnern im Zivil- und Katastrophenschutz Tirols zu den Themen Strom, IKT und Führung. Die Hinweise stammen aus Gesprächen, welche mit allen diesen Partnern am Anfang des Projektes „Ausarbeitung Handbuch Blackout“ durchgeführt wurden. Gerade solche Hinweise aus der Praxis, von Profis mit den unterschiedlichsten Professionen, helfen im Notfall dem einen oder anderen Betroffenen seine Aufgaben leichter zu erfüllen.

Strom**3.4.1****Notstromkreise**

Den Stromkreis für die USV-Versorgung unbedingt klein halten. Am besten einzelne USV-Versorgungsringe immer nur Bauteilweise und Stockweise verlegen. Denn sollte ein Fehler oder unberechtigte Abnahmegeräte den USV-Stromkreis lahm legen, dann ist nicht die ganze USV-Versorgung davon betroffen.

Umschaltung Netzbetrieb / Notstrombetrieb

Die Umschaltung von Netz- auf Notstrombetrieb (USV / Notstromaggregat) ist regelmäßig zu testen, nur dann hat man die Sicherheit, dass es auch im Ernstfall funktioniert. Die Garantie und das Versprechen des Elektrikers bzw. des Technikers, dass ihre Umschaltung auf Notstromversorgung funktioniert, reicht zu diesem Zweck nicht aus – hier ist Vertrauen zuwenig. Halten Sie sich unbedingt an das Motto – „Vertrauen ist gut – testen ist besser!“

Rundfunkinformation bei Stromausfall

Möchte man bei Stromausfall und Kommunikationsausfall weiterhin zumindest Informationen über den Rundfunk erhalten, ist das „alte Kofferradio“ (batteriebetrieben) bzw das Autoradio noch immer das Mittel der Wahl. Stellen Sie die Verfügbarkeit dieser Geräte sicher.

Frequenztoleranz bei Geräten während Netzwiederaufbau

Das Netzwiederaufbaukonzept sieht in Abweichung zum Normbetrieb anstelle der üblichen Frequenz von 50Hz eine höhere Schwankungsbreite der Frequenz von 50,2 – 51,5 Hz im Inselbetrieb vor. Im Extremfall kann die Frequenz kurzzeitig bis 49,2 Hz nach unten und 52,5 Hz nach oben ausschlagen. Geräte und Anlagen, die für das Krisenmanagement gebraucht werden, sollten auf ihre Funktionalität unter diesen Bedingungen überprüft werden.

IKT**3.4.2**

Das permanente Berieseln bzw. die Überflutung der Mitarbeiter mit Informationen im laufenden Normalbetrieb birgt für Notsituationen eine Gefahr in sich. Die Mitarbeiter sind aufgrund dieses automatisierten Informationsprozesses verwöhnt und nicht mehr gewohnt, sich selbst Informationen zu beschaffen. Eine aktive Beschaffung von Informationen gehört aber zu den Aufgaben in einer Notsituation. Hier empfehlen wir im täglichen Betrieb die Einführung der „Holschuld“ der Mitarbeiter. So können beispielsweise Informationen im Intranet zur Verfügung gestellt werden, die jeder Mitarbeiter sich selbst holen muss. So können Mitarbeiter geschult werden, sich aktiv um Informationen zu kümmern.

Krisenkommunikationsmittel

Für die Krisenkommunikation steht den Partnern im Zivil- und Katastrophenschutz die Internetplattform ESIS in Tirol zur Verfügung. Dieses Mittel ist im Ernstfall voll zu nutzen. Durch Einsatz von weiteren Kommunikationsmitteln wie Fax, E-Mails, mündliche Benachrichtigungen usw. steigt die Wahrscheinlichkeit, dass Informationen falsch bzw. vollständig übermittelt werden. Damit ESIS im Ernstfall richtig genutzt werden kann, wird empfohlen, sich mit den Möglichkeiten dieses Systems vertraut zu machen und die Bedienung regelmäßig zu üben.

Notbetrieb ohne PC

Bei einem IKT-Komplettausfall kann der interne Informationsfluss mit Bleistift und Zettel aufrechterhalten werden. Diese Arbeitsweise wird als „organisierter Betriebszustand“ bezeichnet und benötigt einen rund 2/3 höheren Personaleinsatz als der Normalbetrieb mit dem PC. Wichtig – dieses Verfahren ist vorab festzulegen und zu üben.

Akkus

Für batteriebetriebene Geräte (z.B. Mobiltelefone, Funkgeräte, Radiogeräte) müssen stets geladene Ersatzbatterien oder Akkus bereitgehalten werden. Damit die Akkus auch bei Netzstromausfall aufgeladen werden können, sind Ladevorrichtungen, welche an Notstromaggregaten oder Fahrzeugen angeschlossen werden können, bereitzuhalten.

Tipps bei Handyverbindungsproblemen

Kein Netz?

- Empfang suchen, nochmals probieren
- Im Notfall können ausländische SIM-Karten Verwendung finden, da diese automatisch auf noch funktionierende Netze zugreifen. Zu beachten dabei: das verwendete Handy muss entsperrt und somit für fremde SIM-Karten zugänglich sein. Bei Verwendung von ausländischen Wertkarten ist auf deren Ablaufregelung zu achten. Ausländische SIM-Karte einlegen und einschalten.

Netz dauernd belegt?

- Nicht alle paar Sekunden Sendetaste drücken, einige Minuten abwarten und erneut probieren – unnötige Signalisierungslast im Netz vermeiden
- SMS senden – evtl. mit Empfangsbestätigung
- UMTS Netz manuell wählen

Nichts geht?

- Euronotruf 112 – verdrängt normale Gespräche. Denn in jenen Fällen, in denen das eigene Netz nicht verfügbar ist, kann in Notfällen möglicherweise mit der europäischen Notrufnummer 112 eine Verbindung über einen anderen Netzbetreiber aufgebaut werden.
Die Nummer 112 funktioniert mit und ohne SIM-Karte.
- Handy ausschalten, nach Einschalten statt PIN-Eingabe gleich 112 wählen. In Tirol antwortet die jeweilige Bezirksleitzentrale der Polizei, in Grenzgebieten die Notrufzentralen der angrenzenden Länder.
- Satellitentelefon als Alternative zu Festnetz- und Mobiltelefon in Betrieb nehmen.
Achtung: Gespräche können nur mit Teilnehmern von funktionierenden Netzen oder anderen Satellitentelefonen geführt werden.

Üben, üben, üben...

Führen besteht darin, Information einzuholen und weiterzuleiten, Entscheidungen zu treffen und diese weiterzuleiten und deren Umsetzung zu kontrollieren.

Dies muss im äußersten Notfall auch mit „Bleistift und Papier“ erfolgen können.

Damit dies auch klappt, sind diese Vorgänge regelmäßig zu üben.

Dadurch werden alle sensibilisiert. Beim Üben dürfen und sollen Fehler anfallen. Durch einen eingeleiteten Verbesserungsprozess wachsen die Beteiligten gerade daran und die Angst und Unsicherheit wird ihnen genommen.

Die Sensibilisierung durch regelmäßige Übungen trägt dazu bei, frühzeitig außerordentliche Gefahren zu erkennen, um dementsprechend rechtzeitig zu reagieren.

Beispielsweise kann bei einer kritischen Wetterprognose bereits mit persönlichen Vorbereitungen begonnen werden. Handy aufladen, Kraftfahrzeug tanken, Einsatzvorbereitungen treffen, sich bereithalten usw.

4.1 Inhalt des Einsatzplanes

4.1.1 Führungsorganisation

Darstellung der Führungsorganisation

Die Führungsorganisation ist schriftlich und grafisch darzustellen. Klar hervorgehen müssen die Hierarchien, die einzelnen Funktionen, deren Aufgaben und Kompetenzen.

Beschreibung des Führungsverfahrens

Kurz beschrieben oder grafisch dargestellt wird hier das zur Anwendung kommende Führungsverfahren zur Erstellung, Übermittlung und Kontrolle von Handlungsanweisungen durch die Führungsorganisation.

Auflistung von Führungsmitteln

Die zur Verfügung stehenden Führungsmittel sind aufzulisten. Der Aufbewahrungsort ist anzugeben.

4.1.2 Alarmorganisation

Definition von Alarmstufen

Zur Anpassung und Vereinfachung der Vorgangsweise an die unterschiedlichen Schweregrade von möglichen Ereignissen sind Alarmstufen festzulegen.

Die Gliederung erfolgt ausgehend vom Normalzustand über Vorwarnstufen bis hin zum größtmöglich anzunehmenden Ereignis. Mehr als fünf Alarmstufen sollten der Einfachheit und Übersichtlichkeit wegen nicht festgelegt werden.

Aufstellung des Alarmplanes

Im Alarmplan ist für jede einzelne Stufe die Alarmierung festzulegen. Alle nach Auslösung dieser Stufe zu verständigenden Behörden, Organisationen, Funktionen und Personen werden aufgelistet und grafisch dargestellt.

4.1.3 Einsatzszenarien

Ausarbeitung von Checklisten

Für alle möglichen Einsatzszenarien sind Handlungsanweisungen bzw. -optionen für die Führungsorganisation auszuarbeiten und in Form von übersichtlichen Checklisten darzustellen. Wichtige Informationen sind in Text oder in grafischer Form beizulegen.

4.1.4 Listen und Verzeichnisse

Ressourcenverzeichnisse

Ressourcenverzeichnisse sind Verzeichnisse, welche interne und externe Ressourcen, die im Einsatzfall benötigt werden, enthalten.

Telefonlisten

Telefonnummern und andere Erreichbarkeiten, welche im Einsatzfall benötigt werden, sind in den Telefonlisten festzuhalten.

4.2 Vorgangsweise

Für die Ausarbeitung eines Einsatzplanes wie er hier beschrieben und empfohlen wird, sollte innerhalb der eigenen Organisation ein Verantwortlicher ernannt und mit den erforderlichen Kompetenzen ausgestattet werden. Zusätzlich müssen Zeit, Mittel und wo erforderlich Fachkompetenz zur Verfügung stehen. Einsatzpläne funktionieren nur, wenn diese praxisnahe, präzise und auf realistischer Basis erstellt und entsprechend implementiert werden.

„Implementieren“ bedeutet:

- Alle Personen, welche mit dem erstellten Einsatzplan arbeiten sollen, müssen über den Inhalt vollständig informiert werden und ihre Aufgaben genau kennen.
- Alle im Plan genannten Mittel und Strukturen müssen im Einsatzfall jederzeit zur Verfügung stehen und zugänglich sein.
- Begleitend zur Schulung über die Inhalte des Planes müssen diese Personen in den Bereichen Führen unter Druck, Entscheiden in schwierigen Situationen und Umgang mit Stress in der Führungsorganisation geschult werden.

Schritt 1: Aufbau und Darstellung der Führungsorganisation

Die Führungsorganisation ist schriftlich und grafisch darzustellen. Klar hervorgehen müssen die Hierarchien, die einzelnen Funktionen, deren Aufgaben und Kompetenzen.

Das gesamte Kapitel 1.3 lesen, dann die Checklisten zur Einsatzvorbereitung im Kapitel 2.3 ausfüllen und abschließend im Kapitel 3 die Punkte „3.3.1 Aufbau einer Führungsorganisation“ und „3.3.2 Praktische Vorgangsweise durchlesen.“

In ihrer Organisation entscheiden ob:

1. Eine Führungsorganisation nach den Richtlinien des SKKM neu aufgebaut, oder
2. die bestehende Führungsorganisation diesen Richtlinien angepasst, oder
3. eine eigene Form der (bereits bestehenden) Führungsorganisation gewählt wird.

Bei Umsetzung der Punkte 1 oder 2 die Führungsorganisation gemäß Richtlinien aufstellen. (Richtlinien bei Landeswarnzentrale Tirol erhältlich)

Bei Wahl einer anderen Form laut Punkt 3 diese Organisationsform beschreiben und grafisch darstellen.

In Folge

- auf eine klare Stellvertreterregelung für alle Positionen achten
- die Kompetenzen für die Führungspositionen schriftlich festlegen und
- Checklisten mit den Aufgaben für jede Position erstellen

Schritt 2 : Beschreibung des Führungsverfahrens

Das anzuwendende Führungsverfahren soll kurz beschrieben werden. Festzulegen ist dabei, wie und auf welcher Basis (aktuelle Lageinformationen, Einsatzpläne, Notprozeduren, Anweisungen übergeordneter Stellen usw.) Entscheidungen gefällt und Handlungsanweisungen an nachgeordnete Stellen übermittelt werden. Schließlich ist zu planen, wie die Umsetzung der Handlungsanweisungen kontrolliert wird.

Die Darstellung des Führungsverfahrens durch Anpassung der Grafik im Kapitel 1.3, Seite 56 auf die eigene Organisation wird empfohlen.

Schritt 3: Bestimmung und Auflistung der Führungsmittel

Im Kapitel 1.3 den Punkt 1.3.1.3 Führungsmittel lesen.

Zuerst die erforderlichen Strukturen (Gebäude, Nachrichten- und Sitzungsräume) bestimmen.

Die Strukturen auflisten und zwar mit genauen Angaben wie Adresse, Zugänglichkeit auch außerhalb von Dienstzeiten und den Verantwortlichen für die Inbetriebnahme mit entsprechenden Erreichbarkeiten rund um die Uhr.

Grundrisse der Führungsstrukturen zeichnen und die Zweckbestimmungen der einzelnen Bereiche darstellen.

Dann die erforderlichen Führungsmittel festlegen.

Dies bedarf einer eingehenden Analyse und ist mit einigem Aufwand verbunden. Größter Wert ist dabei auf eine hervorragende Ausstattung zur Informationsbeschaffung, zur Lagedarstellung und für die Kommunikation zu legen. Die Führungsmittel tabellarisch auflisten, den Aufbewahrungsort exakt angeben und wo erforderlich eine kurze Bedienungsanleitung erstellen. Die Kurzbedienungsanleitung nach der tabellarischen Auflistung dem Einsatzplan beilegen.

Schritt 4: Definition der Alarmstufen

Voraussetzung für rasches und sicheres Agieren einer Organisation in Notsituationen ist ein gut gemachter Alarmplan. Ein Alarmplan basiert auf Alarmstufen. Alarmstufen gehören genau definiert. Dafür sind Schwellenwerte so zu beschreiben, dass bei Eintritt von Ereignissen diese zweifelsfrei einer beschriebenen Alarmstufe zugeordnet werden können. Die Anzahl der Alarmstufen sollte ein angemessenes Handeln ermöglichen.

Gegliedert werden können Alarmstufen in zwei Kategorien:

1. Ereignis kann eintreten
Voralarm , Vorbereitung möglich
2. Ereignis eingetroffen
Alarm - Aktion bzw. Handlung dringend erforderlich

Schritt 5: Aufstellung des Alarmplanes

Nach Definition der Alarmstufen kann der Alarmplan ausgearbeitet werden. Dazu ist es nötig, allen Alarmstufen die Funktionen, interne Organisationseinheiten bzw. Dienste oder Teile zuzuordnen, welche bei Erreichung der jeweiligen Stufe zu verständigen sind. Der Alarmplan ist in zwei Teile zu gliedern:

1. Eine grafische Übersicht mit Zuordnung der Funktionen, Dienste oder Organisationseinheiten unterhalb der entsprechenden Alarmstufe
2. Eine Verständigungsliste je Alarmstufe mit Namen und Telefonnummern bzw. sonstigen Erreichbarkeiten

Schritt 6: Ausarbeitung der Checklisten

Für alle zu erwartenden Szenarien sind Checklisten mit Handlungsanweisungen bzw. Handlungsoptionen auszuarbeiten. Checklisten sind klar zu strukturieren und kurz zu fassen. Die aufgelisteten Anweisungen bzw. Optionen innerhalb eines Szenarios sind nach den Alarmstufen zu ordnen:

Szenario A,

Alarmstufe 1 – entsprechende Anweisungen

Alarmstufe 2 – entsprechende Anweisungen usw.

Szenario B

Alarmstufe 1 – entsprechende Anweisungen

Alarmstufe 2 – entsprechende Anweisungen

Für die Festlegung der Szenarien sind Risiko- bzw. für diesen Zweck viel besser geeignet Schadensrelevanzanalysen zu erstellen.

Die daraus ausgearbeiteten Checklisten sind in den Einsatzplan so einzuordnen, dass sie leicht zu finden sind.

Schritt 7: Anlegung der Verzeichnisse und Listen**Ressourcenverzeichnis**

Alle internen und externen Ressourcen, die im Einsatzfall benötigt werden könnten, sind in diesem Verzeichnis aufzulisten. Anzuführen sind Adressen, Telefonnummern und weitere Erreichbarkeiten interner Abteilungen, Personen, Firmen, Dienstleister, Behörden und Organisationen, welche über diese Ressourcen verfügen.

Telefonlisten

Alle im Einsatzfall erforderlichen Festnetznummern, Handynummern, Adressen und anderen Erreichbarkeiten von Personen, Behörden, Organisationen, Firmen, Dienstleister u.a. sind in dieser Liste alphabetisch zu ordnen und aktuell zu halten.

Schritt 8: Verfügbarkeit des Einsatzplanes**Vorhaltung Einsatzplan**

Einsatzpläne sind mehrfach redundant vorzuhalten. Dies kann digital und muss in Papierform erfolgen. Der Einsatzplan muss an bestimmten, den zuständigen Personen bekannten Stellen, immer zur Verfügung stehen.

Aktualisierung Einsatzplan

Hier soll unterschieden werden:

1. schnelllebige Daten (Ressourcen und Telefonverzeichnisse)
Diese müssen von beauftragten Personen ständig aktuell gehalten werden.
Neben der laufenden Aktualisierung bei bekannten Änderungen sollten diese halbjährlich überprüft werden.
2. Inhaltliche konzeptuelle Anpassungen und Änderungen
Diese werden bei Änderung von äußeren Umständen oder bei internen Veränderungen, welche Auswirkungen auf den Notfallplan haben, erforderlich.
Diese Anpassungen sollten von fachkundigen Personen vorgenommen werden.

5.1 Historische Ausfallereignisse

5.1.1 Detaillierte Beschreibung

LAND	DATUM	URSACHE	FOLGEN	DAUER
Nordosten der USA, Teile Kanadas	09.11.1965	defektes Strom-Relais in Ontario (Kanada)	30 Millionen Menschen betroffen. Es wurde befürchtet, dass aufgrund des Kalten Kriegs ein Atomkrieg die Ursache gewesen sei.	12 Stunden
New York City und Gebiete des Landkreises Westchester nördlich von New York	13.07.1977	Blitzeinschläge	Plünderungen und Unruhen Festnahmen von 3800 Menschen Bekämpfung von über 1000 Feuern	24 Stunden
Frankreich	19.12.1978		80% der Fläche Frankreichs betroffen	
England	15.-16.10.1987	Sturm	durch Sturm 23 Tote einige hunderttausend Menschen ohne Strom	bis zu 14 Tagen
Quebec, Kanada	13.03.1989	geomagnetischer Sturm	6 Millionen Menschen ohne Strom	9 Stunden
9 Staaten im Westen der USA Teile Mexikos	11.08.1996	Hitze	einige Millionen Menschen ohne Strom	
Malaysia	03.08.1996		Gesamte malaysische Halbinsel samt der Hauptstadt Kuala Lumpur ohne Strom	
Regionen Ontario, Quebec und Nova Scotia (Kanada) New York und Maine (USA)	04.-10.01.1998	Eissturm	Vier Millionen Menschen ohne Strom 700.000 Menschen nach drei Wochen noch ohne Strom 25 Tote 1000 Stahl-Strommasten und 35.000 Holzmasten zerstört	über 3 Wochen

LAND	DATUM	URSACHE	FOLGEN	DAUER
Gewerbegebiet von Auckland, Neuseeland	01.-02.1998	Hitze und trockene Witterung, veraltete Leitungssysteme	74.000 Betroffene Beschäftigte in diesem Gewerbegebiet 60.000 Personen mussten zuhause oder in anderen Teilen Neuseelands oder Australiens für 5 Wochen arbeiten große Verluste für viele Einzelunternehmen	über 5 Wochen
San Francisco (USA)	08.12.1998	falsches Leistungsmanagement	350.000 Kunden von PG&E ohne Strom wirtschaftlicher Schaden von etwa 10 Millionen Dollar	8 Stunden
Quebec, Kanada	04.-05.07.1999	Wirbelsturm	70 Verletzte 4 Tote mehr als 100 Millionen Dollar Schaden 700.000 Haushalte und Firmen ohne Strom.	
Taiwan	29.07.1999	Erdrutsch knickt einen Strommasten einer Hauptversorgungsleitung	8,46 Millionen Menschen ohne Strom	
Kalifornien	2000 und 2001	künstlich herbeigeführte Stromknappheit (Manipulation des freien Marktes)	immer wieder Stromausfälle in kleineren und größeren Gebieten Kaliforniens	
Nordosten der USA sowie Teile Kanadas	14.08.2003	schlechte Wartung der Leitungsnetze	50 Millionen Menschen ohne Strom	einige Stunden bis zu 3 Tagen
London	28.08.2003	Probleme mit einer Hauptversorgungsleitung	500.000 Menschen ohne Strom 400 Notrufe, 100 Personen aus Liften befreit 60% der U-Bahnlinien betroffen	34 Minuten bis zu 2 Stunden
Malaysia	02.09.2003		5 der insgesamt 13 Staaten inklusive Kuala Lumpur ohne Strom	5 Stunden

LAND	DATUM	URSACHE	FOLGEN	DAUER
9 US-Staaten sowie Ontario, Kanada	19.09.2003	Hurrikan Isabel	4,3 Millionen Menschen ohne Strom	
Südschweden und Dänemark	24.09.2003	Unwetter Reparaturarbeiten in dem schwedischen Kernkraftwerk Oskarshamn	3,5 Millionen Menschen ohne Strom Viele Unfälle infolge ausgefallener Ampelanlagen Stillstand der Eisenbahnen Ausfall der Telefone	einige Stunden
Italien	28.09.2003	Menschliches Versagen Kommunikationsprobleme Trigger: Erdschluss einer Leitung in der Schweiz	Gesamtstaatliches Blackout 5 Todesopfer 1 Mrd. Euro Schaden 56 Millionen Menschen betroffen 120.000 Personen betroffen	Südlicher Teil Italiens bis zu 2 Tagen
San Francisco	20.12.2003			
Athen und Umgebung	12.07.2004	Spannungskollaps: zunehmende elektrische Last durch zunehmende Klimatisierung		
Florida (USA)	04.09.2004	Hurrikan Frances	5 Millionen Menschen ohne Strom	
Puerto Rico	15.09.2004	Regierung beschloss Stromabschaltung aufgrund Hurrikan Jeanne	100 Millionen US-Dollar Schaden 3 Tote	
Schweden	08.01.2005	Sturm Erwin	341.000 Haushalte ohne Stromversorgung	einige Tage bis zu mehr als 3 Wochen
Moskau	25.05.2005		10 Millionen Menschen	24 Stunden
Puerto Rico	16.06.2005	Ausfall einer 250-kV-Leitung	2/3 der Bevölkerung von Puerto Rico betroffen	1 Nacht

LAND	DATUM	URSACHE	FOLGEN	DAUER
Schweiz	22.06.2005	falsches Kraftwerks und Leistungsmanagement	200.000 Pendler steckten in rund 1500 Zügen fest.	drei Stunden
Java-Insel, Indonesien	18.08.2005	Energieengpass	100 Millionen Menschen betroffen	7 Stunden
Bagdad, Basra, UmmQasr (Irak)	22.08.2005	Sabotage	Süd- und Zentral-Irak inklusive Bagdad ohne Strom Basra ohne Strom Umm Qasr (einziger Hafen im Irak) ohne Strom	7 Stunden
Florida	26.08.2005	Hurrikan Katrina	1,3 Millionen Menschen ohne Strom	4 Tage bis zu einer Woche
Louisiana, Mississippi, Alabama	29.08.2005	Hurrikan Katrina	mehrere Millionen Menschen ohne Strom	bis zu einigen Wochen
Los Angeles	12.09.2005	falsches Leistungsmanagement	mehrere Millionen Menschen ohne Strom	1,5 Stunden
Florida	24.10.2005	Hurrikan Wilma	6 Millionen Menschen ohne Strom	bis zu 3 Wochen
Österreich	30.10.2005	technische Probleme	Ausfall von ca. 400 der österreichweit 4.000 Bankomaten	einige Stunden
Norden von Nordrhein-Westfalens sowie Teile von Südwest-Niedersachsen	25.11.2005	heftige Schneefälle	250.000 Menschen betroffen wirtschaftlicher Schaden von 100 Millionen Euro	bis zu 3 Tagen
Auckland, Neuseeland	12.06.2006	Defekt in einem Umspannwerk, verursacht durch heftige Windböen	230.000 Stromkunden (700.000 Bewohner) betroffen Ausfall der Eisenbahn Ausfall über 300 Ampelanlagen Sperrung einiger Spitäler	8 Stunden
einige Bundesstaaten der USA und Quebec, Kanada	17.-21.07.2006	Wirbelstürme	3 Millionen Personen ohne Strom	bis zu einigen Wochen
Queens, New York, USA	18.-24.07.2006	Hitzewelle	50.000 Kunden von Con Edison ohne Strom La Guardia Airport: 45 Flüge gecancelled, 11 Flüge umgeleitet Ausfälle im Bereich der U-Bahnen	bis zu einer Woche

LAND	DATUM	URSACHE	FOLGEN	DAUER
Philadelphia	18.07.2006	Sturm	365.000 Kunden ohne Strom 2 Tote Millionenschäden	einige Tage
St. Louis, Missouri	19.07.2006	Wirbelstürme	600.000 Menschen ohne Strom 2/3 des Lambert - St. Louis International Airport ohne Strom	bis zu 9 Tagen
London	22.07.2006	Hitzewelle, großer Bedarf an Strom	Teile Londons ohne Strom	bis zu 1 Tag
Quebec, Kanada	01.08.2006	Wirbelstürme	Provinz Quebec: 146.000 Haushalte stromlos. inklusive Großraum Montreal: 450.000 Haushalte betroffen	bis zu 1 Tag
Süd- und Ost-Ontario, USA	02.08.2006	Wirbelstürme	250.000 Haushalte betroffen	einige Tage
London	12.09.2006		Teile von London ohne Strom	kurzfristig
Lima, Peru	24.10.2006	Ballon	13 Bezirke von Lima ohne Strom	einige Stunden
Teile von Deutschland, Frankreich, Belgien, Italien, Österreich, Spanien und Marokko	04.11.2006	falsches Leistungsmanagement	zehn Millionen Haushalte in Europa Bahnverkehr wurde massiv beeinträchtigt	einige Stunden
British Columbia, Kanada	15.11.2006	Stürme	200.000 Haushalte ohne Strom	bis zu einer Woche
St. Louis, Missouri, USA	01.12.2006	Wintersturm	350.000 Haushalte ohne Strom	einige Stunden
Ontario	01.-02.12.2006	Wintersturm	einige zehntausend Personen ohne Stromversorgung	bis zu 2 Tagen
Seattle, USA	15.12.2006	Wintersturm	1 Million Menschen ohne Strom	bis zu 5 Tagen

LAND	DATUM	URSACHE	FOLGEN	DAUER
Queens, New York, USA	18.-24.07.2006	Hitzewelle	50.000 Kunden von Con Edison ohne Strom La Guardia Airport: 45 Flüge gecancelled, 11 Flüge umgeleitet Ausfälle im Bereich der U-Bahnen	bis zu einer Woche
Teile der USA und Kanadas	12.-24.01.2007	Winter- und Eisstürme	1,5 Millionen Kunden ohne Strom	bis zu 5 Tagen
State of Victoria, Australien	16.01.2007	Buschfeuer	200.000 Menschen ohne Strom öffentliche Verkehrsmittel in Melbourne betroffen 1.200 Ampeln in Melbourne und Vororten ausgefallen	bis zu einem Tag
Costa Rica	19.04.2007		gesamtnationaler Stromausfall 4,3 Millionen Menschen betroffen	1,5 Stunden
Kolumbien	26.04.2007	technischer Fehler in Umspannwerk	80 % Kolumbiens betroffen	einige Stunden
New York, USA	27.06.2007		136.700 Kunden betroffen	eine Stunde
Barcelona und Vororte, Spanien	23.07.2007	Feuer in drei Umspannwerken	Vororte Barcelonas ohne Strom	bis zu 78 Stunden
Mazedonien, Albanien und Teile Griechenlands	25.07.2007	Hitzewelle	Teile dieser Länder ohne Strom	bis zu einem Tag
Österreich	07.08.2007	Stromausfall nach Störung durch Bohrarbeiten	Ausfall der Telefonanlage in einem Krankenhaus in Eisenstadt. Das Krankenhaus war für ca. 2 Stunden nur über Mobiltelefone erreichbar	einige Stunden
Österreich	16.01.2008	Leistungsprobleme	Ausfall des A1-Breitbandes in Niederösterreich	einige Stunden
	Jänner 2008	Trojaner	Auftreten einer Welle von Attacken, die offensichtlich gegen Exilbürger gerichtet waren, mittels Trojanern, welche eine bis dahin unbekannte Sicherheitslücke ausnutzten. Neben Diebstahl von Informationen können auch gezielt Webseiten gecrackt, Systeme gestört und außer Funktion genommen werden.	

Anhang:	5.2
Informationsformulare Landeswarnzentrale	

1. Erhebung Führungsorganisation	5.2.1
---	--------------

Zur Sicherstellung der Interoperabilität zwischen den einzelnen Partnern im Zivil- und Katastrophenschutz ersuchen wir Sie, die aktuelle Organisationsform Ihrer Führungsorganisation bei Netzstrom- und IKT-Ausfällen mitzuteilen.

Wenn Ihre Führungsorganisation gemäß Richtlinie SKKM oder in ähnlicher Form aufgebaut ist, kreuzen Sie bitte in Spalte 1 die bei Ihnen in Verwendung stehenden Funktionen an. Ist Ihre Führungsorganisation in anderer Form strukturiert, tragen Sie bitte die bei Ihnen in Verwendung stehende Bezeichnung für die Führungsfunktion und jene für andere Funktionen in den entsprechenden Zeilen der Spalte 2 ein.

Bitte geben Sie noch an, ob der Führungsstab fix an einem Tagungsort gebunden ist, oder ob der Stab mobil einsetzbar ist.

2. Erhebung Kommunikationsmittel – KT	5.2.2
--	--------------

Damit die Kommunikation auch bei Ausfällen zwischen den Partnern im Zivil- und Katastrophenschutz sichergestellt werden kann, bitten wir Sie, Ihre Kommunikationsgeräte und -einrichtung aufzulisten.

Es wird ersucht, in der Spalte die Ihnen zur Verfügung stehenden Geräte und Einrichtungen einzutragen, z.B.: Festnetztelefon, Mobiltelefon, Funk, E-Mail, Internet, usw. In der Spalte Kennung bitten wir Sie die entsprechenden Telefonnummern, Funkrufnamen mit Angabe von Kanal und Frequenz, E-Mail-Adressen usw. einzutragen.

Im untersten Feld bitte angeben, ob Ihre Organisation, Einrichtung oder Behörde über eine ständig besetzte Stelle oder eine Rufbereitschaft verfügt. Ergänzen Sie diese Angabe mit der Erreichbarkeit (Telefonnummer, Adresse).

Die Angaben werden streng vertraulich behandelt.

Nach Abschluss der Erhebungen wird ein Kommunikationsplan erstellt und nach Freigabe der eigenen Daten durch jeden einzelnen Partner allen zur Verfügung gestellt.

Partner im Zivil- und Katastrophenschutz

Organisation / Behörde / Institution	
Adresse	
Ansprechpartner	
Telefon / E-Mail / Telefax	

Derzeitige Organisationsform Führungsstab

Führungsstab gemäß Richtlinie SKKM*			Eigene Organisationsform
Einsatzleiter <input type="checkbox"/>			Bezeichnung leitende Funktion
Leiter Stabsarbeit <input type="checkbox"/>			
Führungsstab S1-S6			Bezeichnung weiterer Funktionen
S1	Personal – Innerer Dienst	<input type="checkbox"/>	
S2	Lage	<input type="checkbox"/>	
S3	Einsatz	<input type="checkbox"/>	
S4	Versorgung	<input type="checkbox"/>	
S5	Presse - Medien	<input type="checkbox"/>	
S6	Information - Kommunikation	<input type="checkbox"/>	
Fachexpertenstab <input type="checkbox"/>			

Tagungsort Führungsstab	nur im Haus	<input type="checkbox"/>
	auch mobil, außer Haus	<input type="checkbox"/>

*Richtlinie des staatlichen Krisen- und Katastrophen - Managements zur Vereinheitlichung der Führungsorganisation im Krisen- und Katastrophenfall.
Die Richtlinie kann in der Landeswarnzentrale Tirol angefordert werden.

Organisation / Firma / Institution	Anrede	Vorname	Nachname	Funktion	Telefongeschäftlich	Mobiltelefon	E-Mail-Adresse	Faxgeschäftlich	Straße	Ort	Postleitzahl
ARZ Ibk.		Waldemar	Lindner	Innenorganisation	+43 504009 1310		waldemar.lindner@arz.co.at		Anton-Melzer-Straße 11	Innsbruck	6020
ASFINAG	DI	Dietmar	Harbauer	Abt. Elektrom. Erhaltung	+43 5010818510	+43 6646010818510	dietmar.harbauer@asfinag.at	+43 5010818020	Rennweg 10 a		
Austro Control		Herwig	Deutinger	Flugsicherung Innsbruck	+43 51222525 500		herwig.deutinger@austrocontrol.at	+43 51706656	Fürstenweg 180	Innsbruck	6020
Austro Control	Ing.	Ernst	Wieser	Leiter Flugsicherung Innsbruck	+43 51703 6612		ernst.wieser@austrocontrol.at		Fürstenweg 180	Innsbruck	6020
Austro Control	Ing.		Kleinlerchner	Leiter Technik	+43 51703 5660				Fürstenweg 180	Innsbruck	6020
				Warn- und Alarmsystem,							
BOS	Ing.	Alois	Angerer	Behördenfunk, Digitalfunk;	+43 5125082267		alois.angerer@tirol.gv.at		Herrngasse 1-3	Innsbruck	6010
Datenverarbeitung Tirol GmbH		Werner	Cicatka	Leitung Rechenzentrum	+43 5125083345	+43 512508883345	werner.cicatka@tirol.gv.at	+43 5125083355	Adamgasse 22	Innsbruck	6020
Flughafen Innsbruck	DI	Marco	Pernetta	Flughafenbetriebsleiter	+43 51222525100	+43 6644422115	marco.pernetta@innsbruck-airport.com	+43 51222525102	Fürstenweg 180	Innsbruck	6020
Integrierte Landesleitstellen GmbH	Ing.	Gernot	Vergeiner	Geschäftsführer	+43 5123313301	+43 6642445115	gernot.vergeiner@leitsstelle-tirol.at	+43 512361444	Eduard Bodem Gasse 2/3	Innsbruck	6020
Land Tirol Landeswarnzentrale	Ing. MBA MPA	Marcel	Innerkofler	Leiter Landeswarnzentrale	+43 51258058015	+43 676885082272	marcel.innerkofler@tirol.gv.at	+43 512589368	Eduard-Wallnöfer-Platz 3	Innsbruck	6020
Land Tirol Landeswarnzentrale	Ing. MBA	Stefan	Thaler	Stv. Leiter Landeswarnzentrale	+43 51258058016	+43 676885082273	stefan.thaler@tirol.gv.at	+43 512589368	Eduard-Wallnöfer-Platz 3	Innsbruck	6020
Mobilkom	Ing.	Franz	Nigl	Notfallmanager Tirol	+43 5122121000	+43 6643315350	f.nigl@mobilkom.at		Fürstenweg 47	Innsbruck	6020
ORF Landesstudio Tirol	DI	Bernhard	Garber	Techn. Leiter/Produktionsleiter	+43 512534326335		bernhard.garber@orf.at	+43 5125343550382	Rennweg 14	Innsbruck	6010
Österreichische Bundesbahnen		Herbert	Knödl	Leiter Gesamtproduktion	+43 512-503-2346	+43 664-6172160	herbert.knoedl@oebb.at	+43 512-503-57587	Fennerstraße 12	Innsbruck	6020
Österreichisches Bundesheer	ObstLt	Dietmar	Heiss	Militärkommando Tirol/S3	+43 50201 6040300	+43 6648983571	milkdot@bmlv.gv.at	+43 502016017403	General Eccherstraße 2	Innsbruck	6020
Österreichisches Bundesheer	ObstLt	Herwig	Müller	Militärkommando Tirol/S6	+43 50201 6040600	+43 6646225316	milkdot@bmlv.gv.at	+43 502016017400	General Eccherstraße 2	Innsbruck	6020
Landespolizeikommando Tirol	ObstLt	Peter	Platzgummer	Logistik	+43 512-5900-707001	0043 664 1840134	peter.platzgummer@polizei.gv.at	+43 512-5900-707009	Innrain 34	Innsbruck	6010
Telekom		Dietmar	Hauser	Leiter Krisenstab Telekom	+43 59059 5 47001	+43 664 629 5700	dietmar.hauser@telekom.at		Andreas Hofer Straße 26a	Innsbruck	6020
TILAK	Ing.	Günther	Pfaringer	Sicherheit TILAK	+43 51250424440	+43 6643415888	guenter.pfaringer@tilak.at	+43 5125044443			
Tiroler Wasserkraft AG	DI	Walter	Auer	Krisenmanagement	+43 5060721111	+43 69912572111	walter.auer@tiwag.at	+43 5060721284	Eduard-Wallnöfer-Platz 2	Innsbruck	6020
Tiwag Netz	DI	Klaus	Schüller	Systemführung Netze	+43 5070826301	+43 699 12561301	klaus.schueller@tiwag-netz.at	+43 5070826367	Bert-Köllensperger-Str. 7A	Thaur	6065
Verbund AG	Ing.	Heinz	Nyvelt	Betriebsleitung AHP Mayrhofen	+43 5285812725415	+43 6641816138	NyveltH@verbund.at	+43 5285812725314	Tuxerstraße	Mayrhofen	
				Leiter Sicherheits- und							
Sicherheitsdirektion für Tirol	Dr.	Edelbert	Kohler	Kriminalpolizei	+43 512-5900-756200	+43 6648187993	edelbert.kohler@polizei.gv.at	+43 512-5900-756113	Maria-Theresien-Straße 43	Innsbruck	6020

Bezirkshauptleute

Bezirkshauptmannschaft Kufstein	Dr.	Michael	Berger	Bezirkshauptmann	+43 53726066000	+43 676885056000	michael.berger@tirol.gv.at	+43 53726066015			
Bezirkshauptmannschaft Kitzbühel	Dr.	Christoph	Hochenegg	Bezirkshauptmann	+43 5356621316300	+43 676885086300	christoph.hochenegg@tirol.gv.at	+43 5356621316305			
Bezirkshauptmannschaft Lienz	Dr.	Paul	Wöll	Bezirkshauptmann	+43 485266336500	+43 676885086500	paul.woell@tirol.gv.at	+43 485266336505			
Bezirkshauptmannschaft Schwaz	Dr.	Karl	Mark	Bezirkshauptmann	+43 524269315800	+43 676885085800	karl.mark@tirol.gv.at	+43 524269315805			
Bezirkshauptmannschaft Innsbruck Land	Dr.	Herbert	Hauser	Bezirkshauptmann	+43 51253445000	+43 676885085000	herbert.hauser@tirol.gv.at	+43 051253445005			
Bezirkshauptmannschaft Imst	Dr.	Raimund	Waldner	Bezirkshauptmann	+43 54126996	+43 676885085200	raimund.waldner@tirol.gv.at	+43 541269965205			
Bezirkshauptmannschaft Landeck	Dr.	Markus	Maaß	Bezirkshauptmann	+43 54426996	+43 676885085400	markus.maaß@tirol.gv.at	+43 544269965415			
Bezirkshauptmannschaft Reutte	Dr.	Dietmar	Schönnach	Bezirkshauptmann	+43 567269965600	+43 676885085600	dietmar.schoennach@tirol.gv.at	+43 0567269965605			

Bezirkshauptmannschaften

Bezirkshauptmannschaft Kufstein	Dr.	Herbert	Haberl	Katastrophenschutzreferent	+43 53726066290	+43 676885086290	herbert.haberl@tirol.gv.at	+43 53726066015			
Bezirkshauptmannschaft Kitzbühel	Dr.	Martin	Grander	Katastrophenschutzreferent	+43 5356621316430	+43 676885086400	martin.grander@tirol.gv.at	+43 5356621316305			
Bezirkshauptmannschaft Lienz	Dr.	Bert	Singer	Katastrophenschutzreferent	+43 485266336620	+43 6641568115	bert.singer@tirol.gv.at	+43 485266336505			
Bezirkshauptmannschaft Schwaz		Armin	Höfer	Katastrophenschutzreferent	+43 524269315810	+43 676885085810	armin.hoefer@tirol.gv.at	+43 524269315805			
Bezirkshauptmannschaft Innsbruck Land		Klaus	Plattner	Katastrophenschutzreferent	+43 51253445180	+43 676885085180	nikolaus.plattner@tirol.gv.at	+43 51253445185			
Bezirkshauptmannschaft Imst	Mag.	Andreas	Nagele	Katastrophenschutzreferent	+43 541269965270	+43 676885085270	andreas.nagele@tirol.gv.at	+43 541269965215			
Bezirkshauptmannschaft Landeck	Mag.	Siegmond	Geiger	Katastrophenschutzreferent	+43 544269965500	+43 676885085500	siegmond.geiger@tirol.gv.at	+43 544269965415			
Bezirkshauptmannschaft Reutte		Georg	Brunner	Katastrophenschutzreferent	+43 567269965607	+43 676885085607	georg.brunner@tirol.gv.at	+43 567269965605			

Projektleitung

AS Ing. Stefan THALER, MBA Leiter-Stv. Landeswarnzentrale Tirol

Kernteam

Obst Karl-Heinz ABENTUNG, Landespolizeikommando Tirol

Obstlt Dietmar HEISS, MBA, Militärkommando Tirol

ObstDntD Lic. Dr. Volkmar KÄPPL, MSc, Militärkommando Tirol

HR Dr. Edelbert KOHLER, Sicherheitsdirektion Tirol

Obst Herwig MÜLLER, Militärkommando Tirol

Hptm Dipl.-Ing. Dr. Andreas RIESER, Militärkommando Tirol

HR Dr. Herbert WALTER, Vorstand der Abteilung Zivil- und Katastrophenschutz, Land Tirol

AR Ing. Marcel INNERKOFLE, MBA MPA, Leiter Landeswarnzentrale Tirol

Konzeption und Ausarbeitung des Handbuches

SECURPLAN - www.securplan.at

AKKM Anton GÖGELE

AKKM Michael MÖSSINGER, MBA

Daniel SPADA

Franco LAVINA

Lektorat

Monika BRAUN



Von links: Marcel INNERKOFLE, Andreas RIESER, Herwig MÜLLER, Volkmar KÄPPL, Stefan THALER, Edelbert KOHLER, Karl-Heinz ABENTUNG, Anton GÖGELE, Michael MÖSSINGER

Medieninhaber

Land Tirol

Herrengasse 1-3

A-6010 Innsbruck

Telefon: ++43 (0)512/508-2260

Telefax: ++43 (0)512/508-2265

E-Mail: herbert.walter@tirol.gv.at

Internet: <http://www.tirol.gv.at>

© **Land Tirol 2008**

Alle Rechte vorbehalten: Nachdruck oder Vervielfältigung,
Aufnahme auf oder in sonstige Medien oder Datenträger sind
nur mit ausdrücklicher Zustimmung der Landesregierung Tirol gestattet.

Backbone Telekom Austria	Der Backbone der Telekom Austria ist der verbindende Kernbereich, die Grundstruktur des österreichischen Telekommunikationsnetzes mit sehr hohen Datenübertragungsraten (vergleichbar mit den Autobahnen im Verkehrswesen)
Bezirkseinsatzleitung (BEL)	Einsatzleitung auf Ebene der Bezirkshauptmannschaft gemäß Tiroler Katastrophenmanagementgesetz
Blackout	Plötzlicher Ausfall großer Stromnetze auf regionaler und überregionaler Ebene. Ein Blackout ist eine Großstörung in der Stromversorgung.
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
Digitalfunk	Funksystem, welches zur Übertragung von Sprache digitale Zeichen in Form einer Zahlenkolonne einsetzt, die Information mathematisch beschreibt, im Gegensatz zum Analogfunk, der die Sprache in Form einer physikalischen Größe direkt überträgt. Digitalfunk ermöglicht die gleichzeitige Übertragung von Sprache und Daten.
ELWOG	Österreichisches Elektrizitätswirtschafts- und Organisationsgesetz
EPL	Die Engpaßleistung ist die maximale Dauerleistung, die ein Kraftwerk unter Normalbedingungen abgeben kann.
Ersatzmaßnahmen	Eine Leistung wird durch Ersatzmaßnahmen teilweise ersetzt
Externe IT Anbindung	Verbindung über physikalische Kabel oder Funkverbindungen eines lokalen Rechners oder Netzwerkes (LAN) zu anderen Rechnern oder Netzwerken außerhalb des eigenen Systems
Führungsmittel	Instrumentarium zur Gewinnung, Erfassung, Darstellung, Verarbeitung und Übermittlung von Informationen innerhalb eines Führungsstabes
Führungsorganisation	Hierarchisch aufgebaute Organisation mit klarer Rollen- und Kompetenzzuweisung zur Führung von Behörden, Organisationen, Unternehmen und anderen Diensten im Bereich des Zivil- und Katastrophenschutzes
Führungsstab	Der Führungsstab ist der Teil der Führungsorganisation und mit mehreren Personen in leitender Funktion besetzt. Er schlägt grundlegende (taktische) Entscheidungen dem Einsatzleiter vor
Gemeindeeinsatzleitung (GEL)	Einsatzleitung auf Ebene der Gemeinde gemäß Tiroler Katastrophenmanagementgesetz
Grundschutz I(K)T	Maßnahmenbündel in den Bereichen Hard- und Software, Infrastruktur, Personal und Organisation, Kommunikation und Notfallvorsorge mit dem Ziel, die Verfügbarkeit, die Integrität, die Vertraulichkeit von Daten und IKT-Anwendungen sicherzustellen
IKT	Informations- und Kommunikationstechnologie. Sie umfasst alle Bereiche der Informationstechnologie (IT) und der Kommunikationstechnologie (KT).
IKT Anbieter	Dienstleister in einer Sparte im IKT-Bereich, z.B. Mobilfunkanbieter, Provider, Infrastrukturbetreiber
IKT Strukturen	Alle physikalischen Strukturen wie Geräte, Netzwerke, Übertragungsleitungen Zentralrechner usw., die zum Betreiben von IKT-Einrichtungen erforderlich sind
Infrastrukturbetreiber	Unternehmen oder Organisation, welche für die Funktion von IKT-Infrastrukturen verantwortlich sind, z.B. Telekom Austria
Landeseinsatzleitung (LEL)	Einsatzleitung auf Ebene der Landesregierung gemäß Tiroler Katastrophenmanagementgesetz
Landeseinsatzleiter	Einsatzleiter im Katastrophenfall für ganz Tirol gemäß Tiroler Katastrophenmanagementgesetz
LWZ	Landeswarnzentrale Tirol – ständig besetzte Stelle der Abteilung Zivil- und Katastrophenschutz der Tiroler Landesregierung
n-1 Kriterium	Sicherheitskriterium für den Betrieb des europäischen UCTE Stromnetzes: Bei Ausfall eines wesentlichen Betriebsmittels im Stromnetz (Kraftwerk, Hochspannungsleitung, Transformator) darf es zu keiner Überlastung oder gar zu einer Unterbrechung der Stromversorgung kommen.
NEA	Netzersatzanlage – stationäres, fest eingebautes Notstromaggregat das sofort ersatzweise die Stromversorgung bei Netzausfall übernimmt
NEA mobil	Mobile Netzersatzanlage - fahr oder transportfähiges Notstromaggregat, das zum Einsatzort gebracht und angeschlossen werden muss und dann ersatzweise die Stromversorgung bei Netzausfall übernimmt
Netzfrequenz	Mit Netzfrequenz wird in einem Stromnetz die zeitlich konstante Frequenz zur elektrischen Energieversorgung mittels Wechselspannung bezeichnet. Die Netzfrequenz wird in Hz – Hertz gemessen und ist der Indikator zur Regelung der Stromversorgung.
Netzstrom	Elektrische Energie, welche aus dem Netz eines Anbieters zur Verfügung gestellt wird. Der Verbraucher hat dabei keinen Einfluss auf die Versorgungssicherheit.
Notlösung	Eine Leistung wird in geringem Umfang mit anderen Mitteln ersetzt.
Notstrom	Notstrom wird zum Ersatz der Netzstromversorgung bei deren Ausfall gebraucht. Er wird lokal aus Batteriesystemen (USV) oder durch Netzersatzanlagen NEA (Notstromaggregate) zur Verfügung gestellt.
Partner im Zivil- und Katastrophenschutz in Tirol	Behörden und Organisationen mit Sicherheitsaufgaben, Infrastrukturbetreiber und Unternehmen, deren Zusammenarbeit unter einheitlicher Führung der Landeseinsatzleitung zwingend erforderlich ist, um Not- und Katastrophenlagen in Tirol zu bewältigen
Physikalische Infrastruktur IKT	Rechner, Geräte, Anlagen, Leitungen, Kabel, Send- Übertragungs- und Empfangsanlagen, kurzum alle materiellen Teile, welche für die Funktion der Informations- und Kommunikationstechnologie benötigt werden
Redundanz	Eine Leistung wird bei Ausfall des Hauptsystems durch das Vorhandensein funktional gleicher oder vergleichbarer Ressourcen vollständig aufrechterhalten
Sachgebiete S1 – S6	Sachgebiete (Arbeitsbereiche) innerhalb eines Führungsstabes
Technologieplattform	Einheitliche standardisierte Technologie
Telekom Austria JetStream	Highspeed-Multiservice-Netzwerk zur Datenübertragung der Telekom Austria, das die wichtigsten Wirtschaftszentren in Zentral-, Süd- und Südost-Europa verbindet (eine internationale Datenautobahn)
TETRA	TETRA (terrestrial trunked radio), ist ein technischer Standard für digitalen Bündelfunk. Der Digitalfunk BOS Austria in Tirol wird in diesem Standard betrieben.
Traktionsstrom	Strom in der Oberleitung der Eisenbahn, der ausschließlich zum Antrieb und zur Versorgung der Züge verwendet wird.
UCTE	Die Union for the Coordination of Transmission of Electricity, Union für die Koordinierung des Transports von Elektrizität ist der Zusammenschluss von 34 Übertragungsnetzbetreibern aus 22 Ländern. Die UCTE versorgt über das europäische Verbundnetz insgesamt über 400 Millionen Verbraucher. Sie ist für die Sicherheit der Stromversorgung über das europäische Verbundnetz zuständig.
USV	Unterbrechungsfreie Stromversorgung. Sie wird aus Batterien sichergestellt und gewährleistet bei Netzstromausfall den kontinuierlichen Weiterbetrieb von elektrisch betriebenen Geräten und Anlagen.
Vermittlungsstellen	Haupt-, Orts- und Untervermittlungsstellen sind Teil der Telekom Infrastruktur und stellen die notwendigen Verbindungen für Telefongespräche, Fax- und andere Übertragungen über das Telefonnetz her.
Worst Case	Schlechtester oder ungünstigster (anzunehmender) Fall
SKKM Richtlinie	Richtlinie des beim BMI angesiedelten staatlichen Krisen- und Katastrophenmanagements zum Führen im Katastropheneinsatz
Kommunikationsmittel	Im Sinne dieses Handbuchs alle Mittel, welche die Kommunikation zwischen den Partnern im Zivil- und Katastrophenschutz ermöglichen.