

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
6. Januar 2011 (06.01.2011)

(10) Internationale Veröffentlichungsnummer
WO 2011/000627 A1

- (51) **Internationale Patentklassifikation:**
H04L 12/437 (2006.01) H04L 12/40 (2006.01)
H04L 12/24 (2006.01)
- (21) **Internationales Aktenzeichen:** PCT/EP2010/056825
- (22) **Internationales Anmeldedatum:**
18. Mai 2010 (18.05.2010)
- (25) **Einreichungssprache:** Deutsch
- (26) **Veröffentlichungssprache:** Deutsch
- (30) **Angaben zur Priorität:**
10 2009 030 910.1
28. Juni 2009 (28.06.2009) DE
- (71) **Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US):** MINETRONICS GMBH [DE/DE]; Rögeneck 12, 22359 Hamburg (DE).
- (72) **Erfinder; und**
- (75) **Erfinder/Anmelder (nur für US):** MÜLLER, Christoph [DE/DE]; Goethestrasse 52, 49549 Ladbergen (DE).
- (74) **Anwalt:** LIEBETANZ, Michael; Postfach 1772, CH-8027 Zürich (CH).

- (81) **Bestimmungsstaaten** (soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) **Bestimmungsstaaten** (soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Erklärungen gemäß Regel 4.17:

[Fortsetzung auf der nächsten Seite]

(54) **Title:** COMMUNICATION NETWORK AND METHOD FOR SAFETY-RELATED COMMUNICATION IN TUNNEL AND MINING STRUCTURES

(54) **Bezeichnung :** KOMMUNIKATIONSNETZWERK UND VERFAHREN ZUR SICHERHEITSGERICHTETEN KOMMUNIKATION IN TUNNEL- UND BERGWERKSSTRUKTUREN

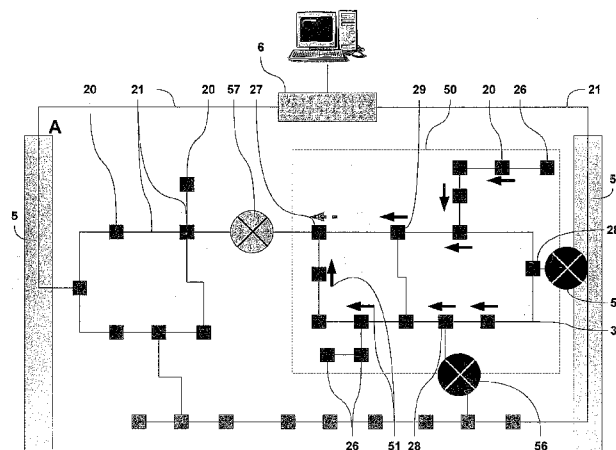


Fig. 3

(57) **Abstract:** The communication network in an underground system (5) comprises a ring network of network computers (20) which is arranged underground, and the network computers are connected to an aboveground central system computer unit (6), each computer having an overview of the overall structure of the ring network and an allocated network status. A multiplicity of these network computers (26, 27, 28) is configured to, in the event of a connection interruption (55, 56, 57) between networked nodes, seek an alternative communication path in order to maintain the communications. A multiplicity of the network computers (20) is provided with or connected to at least one sensor in order to pick up information relating to the environment and being configured to pass on this information to other network computers (20) of the ring network and/or to the aboveground central system (6). In normal operation, the network computers pass on current information relating to the environment to the aboveground central system (6) and to other network computers. In a network island (50) arising as a result of one or more connection interruptions, the network status of a multiplicity of the network computers changes from normal operation to emergency operation,

[Fortsetzung auf der nächsten Seite]



WO 2011/000627 A1



— hinsichtlich der Berechtigung des Anmelders, die Priorität einer früheren Anmeldung zu beanspruchen (Regel 4.17 Ziffer iii)

Veröffentlicht:

— mit internationalem Recherchenbericht (Artikel 21 Absatz 3)

and one of the network computers (29) having the emergency operation network status assumes a master status and all the other networked computers of the network island assume a slave status. Therefore, the network computer (29) having the master status can provide the information relating to the environment in emergency operation to all the other networked computers of the network island, and is also configured to perform network administrative functions of the central system (6) in the network island (50) arising as a result of the connection interruption.

(57) Zusammenfassung: Ein Kommunikationswerk in einem Untertage-System (5) umfasst ein untertage angeordnetes Ringnetzwerk von Netzwerkrechnern (20), welche mit einer übertägigen Zentralsystemrechnereinheit (6) verbunden sind, wobei jeder Rechner einen Überblick über die Gesamtstruktur des Ringnetzwerks hat und einen zugewiesenen Netzwerkstatus hat. Eine Vielzahl dieser Netzwerkrechner (26, 27, 28) ist ausgestaltet, um im Falle eines Verbindungsunterbruchs (55, 56, 57) zwischen Netzknoten zur Aufrechterhaltung der Kommunikation einen alternativen Kommunikationsweg zu suchen, wobei eine Vielzahl der Netzwerkrechner (20) mit mindestens einem Sensor versehen oder verbunden ist, um die Umwelt betreffende Informationen aufzunehmen und ausgestaltet ist, um diese Information an andere Netzwerkrechner (20) des Ringnetzwerkes und/oder an das übertägige Zentralsystem (6) weiterzugeben. Dabei geben die Netzwerkrechner im Normalbetrieb aktuelle die Umwelt betreffende Informationen an das übertägige Zentralsystem (6) sowie an andere Netzwerkrechner weiter. Bei einer Vielzahl der Netzwerkrechner wechselt in einer durch einen oder mehrere Verbindungsunterbrüche entstandenen Netzwerkinsel (50) der besagte Netzwerkstatus von Normalbetrieb auf Notfallbetrieb und einer der besagten Netzwerkrechner (29) mit dem Netzwerkstatus Notfallbetrieb nimmt einen Masterstatus an und alle anderen Netzwerkrechner der Netzwerkinsel nehmen einen Sklavenstatus an. Damit kann der Netzwerkrechner (29) mit dem Masterstatus die besagten die Umwelt betreffenden Informationen im Notfallbetrieb allen anderen Netzwerkrechnern der Netzwerkinsel zur Verfügung stellen und ist auch ausgestaltet, um in der durch den Verbindungsunterbruch entstandenen Netzwerkinsel (50) netzwerkadministrative Funktionen des Zentralsystems (6) zu übernehmen.

TITEL

**Kommunikationsnetzwerk und Verfahren zur sicherheitsgerichteten Kommunikation
in Tunnel- und Bergwerksstrukturen**

5

TECHNISCHES GEBIET

10 Die vorliegende Erfindung betrifft ein Kommunikationsnetzwerk in einem Untertage-Bauwerk, wobei an mehreren Knotenpunkten untertägige Netzwerkrechner angeordnet sind, welche in einem Normalfall jeweils in einer Verbindung zu einer Zentralsystemrechnereinheit stehen, wobei die Netzwerkrechner ausgebildet sind, einen Notfall durch Verlust der Verbindung zu der Zentralsystemrechnereinheit zu erkennen und dann einen Notfallmodus einzuleiten und sie

15 betrifft weiterhin ein Kommunikationselement für ein solches Netzwerk und ein Verfahren zur sicherheitsgerichteten Kommunikation.

STAND DER TECHNIK

20 Kommunikation im Tunnel- und Bergbaubereich findet heute mit Hilfe unterschiedlicher Systemtechnologie statt. Dabei werden für verschiedene Zwecke völlig verschiedene Systeme eingesetzt, wie z.B. Telefon, Datenleitungen („Bussysteme“), Sicherheitssysteme für Gas- und Brandmeldewesen, oder Funkssysteme. Alle diese Systeme müssen separat installiert und

25 unterhalten werden, was in hohen Betriebskosten resultiert.

Es ist das Ziel der Erfindung, die Kommunikation zu vereinheitlichen und damit zu erreichen, dass das Kommunikationssystem im Tagesbetrieb amortisiert werden kann. Darüber hinaus soll es zu minimalen Zusatzkosten auch zur Kommunikation im Notfall dienen und Rettungsteams

30 eine effiziente Kommunikation untereinander und mit der Einsatzleitung ermöglichen. Damit werden die Kosten für Installation und Unterhaltung eines separaten Kommunikationssystems nur für Anwendungen der Grubensicherheit eingespart.

Sogenannte „selbstheilende“ Ringnetzwerke sind beispielsweise aus der EP 0 545 932 und der EP 0 591 429 bekannt.

5

DARSTELLUNG DER ERFINDUNG

Ausgehend von diesem Stand der Technik liegt der Erfindung die Aufgabe zugrunde ein Kommunikationsnetzwerk anzugeben, mit dem die Grubensicherheit erhöht wird.

10 Ferner ist es ein Ziel der vorliegenden Erfindung, ein Verfahren zum Betrieb eines Kommunikationsnetzwerkes anzugeben, mit dem in einem Notfall die Grubensicherheit unterstützt werden kann.

Schliesslich ist es ein Ziel der vorliegenden Erfindung ein Element anzugeben, um zerstörte
15 Verbindungsstrukturen unter Tage in provisorischer Weise sicher wiederherzustellen.

Ein Kommunikationsnetzwerk gemäss der Erfindung ist durch die Merkmale des Anspruchs 1 gekennzeichnet.

20 Ein Kommunikationswerk in einem Untertage-System umfasst ein untertage angeordnetes Ringnetzwerk von Netzwerkrechnern, welche mit einer übertägigen Zentralsystemrechnereinheit verbunden sind, wobei jeder Rechner einen Überblick über die Gesamtstruktur des Ringnetzwerkes hat und einen zugewiesenen Netzwerkstatus hat. Eine Vielzahl dieser Netzwerkrechner ist ausgestaltet, um im Falle eines Verbindungsunterbruchs zwischen
25 Netzknoten zur Aufrechterhaltung der Kommunikation einen alternativen Kommunikationsweg zu suchen, wobei eine Vielzahl der Netzwerkrechnern mit mindestens einem Sensor versehen oder verbunden ist, um die Umwelt betreffende Informationen aufzunehmen und ausgestaltet ist, um diese Information an andere Netzwerkrechner des Ringnetzwerkes und/oder an das übertägige Zentralsystem weiterzugeben. Dabei geben die Netzwerkrechner im Normalbetrieb
30 aktuelle die Umwelt betreffende Informationen an das übertägige Zentralsystem sowie an andere Netzwerkrechner weiter. Bei einer Vielzahl der Netzwerkrechner wechselt in einer durch einen oder mehrere Verbindungsunterbrüche entstandenen Netzwerkinsel der besagte Netzwerkstatus von Normalbetrieb auf Notfallbetrieb und einer der besagten Netzwerkrechner mit dem Netzwerkstatus Notfallbetrieb nimmt einen Masterstatus an und alle anderen Netzwerkrechner

der Netzwerkinsel nehmen einen Sklavenstatus an. Damit kann der Netzwerkrechner mit dem Masterstatus die besagten die Umwelt betreffenden Informationen im Notfallbetrieb allen anderen Netzwerkrechnern der Netzwerkinsel zur Verfügung stellen und ist auch ausgestaltet, um in der durch den Verbindungsunterbruch entstandenen Netzwerkinsel netzwerkadministrative Funktionen des Zentralsystems zu übernehmen.

Ein Verfahren zum Betrieb eines Kommunikationsnetzwerkes ist im Anspruch 9 gekennzeichnet.

Ein vorteilhaftes Element zum Einsatz mit einem Kommunikationswerk zum Aufbau von provisorischen Verbindungsstrukturen ist in Anspruch 11 genannt.

Das Verfahren gemäss der Erfindung vermeidet die Nachteile der traditionellen Kommunikation und setzt auf die Philosophie der Nutzung einer einheitlichen Kommunikation über Ethernet. In diesem vereinheitlichten System werden alle im Tunnel- oder Bergwerksbetrieb anfallenden Daten und Informationen über Netzwerkprotokolle ausgetauscht, wie z.B. Wetterdaten (Ventilationsgeschwindigkeit, Temperaturen, Drücke), Gasinformationen (z.B. CO, CH₄,...), Betriebsdaten, Maschineninformationen, Steuerbefehle, Videoüberwachungsdaten, Sprachkommunikation über PA (Lautsprecheranlagen) oder mit stationären oder mobilen Endgeräten (Telefone), etc.

Um das Datenvolumen aufzuteilen, können basierend auf einer einzigen Technologie verschiedene Netzwerke aufgebaut werden, jedes von ihnen für einen eigenen Zweck, z.B. in Form der Nutzung verschiedener Glasfasern in einem Kabelstrang oder in Form der Nutzung von virtuellen Netzwerken (VLAN's).

Wichtige Vorteile der Technologie liegen in der Nutzbarkeit von netzwerkbasierten Redundanztechnologien wie Ringredundanz oder Meshing.

Ein Kern der Erfindung ist einerseits die Nutzung von Netzwerkinformationen für sicherheitliche Zwecke und andererseits die Nutzung der aktiven Netzwerkkomponenten als aktive Sicherheitsgeräte in Tunneln und Bergwerken oder anderen komplexen Bauwerken, Schiffen etc.

Dabei steht die Nutzung eines vermaschten oder ringförmig aufgebauten Netzes unter Tage als

„Sensor“ für die Intaktheit des Grubengebäudes im Vordergrund, indem z.B. ein plötzlicher Verbindungsverlust Aufschluss über mögliche Unglücksorte bietet.

5 Zudem funktioniert das untertägige Netzwerk als dynamisches, situationsabhängiges Sicherheitssystem. Dieses erstellt, basierend z.B. auf den Informationen aus dem „Sensor“ zusammen mit anderen sicherheitsrelevanten Informationen (z.B. Gas- oder Ventilationsdaten) dynamische Verhaltensregeln an die Mitarbeiter, die sich im Bereich der sich durch Unterbrechungen bildenden „Netzwerkinseln“ befinden. Dazu nutzen die Geräte auch
10 Informationen, z.B. über die Lokalitäten von Notausgängen, Feuerlöschern, Rettungskammern etc., welche im Normalbetrieb auf die einzelnen Netzwerkgeräte heruntergeladen wurden. Diese Informationen werden dann entweder über Displays am Gerät, über vorhandene Displaygeräte wie PC's oder TV-Monitore oder per Funk auf die mobilen Geräte der Mitarbeiter weitergegeben.

15 Dabei verfügt jeder der Netzknoten untertage über ein logisches Abbild des Netzwerkes und über die Zustände (Stati) der einzelnen Verbindungen. Die Ring- oder Mehrfachredundanz sorgt dabei für eine hohe Ausfallsicherheit. Gleichzeitig hat jeder Netzknoten Zugriff auf Umweltinformationen (Luftgeschwindigkeiten, Gasmessungen etc.), welche über das Netzwerk ausgetauscht werden.

20 Wenn etwas Aussergewöhnliches passiert, (z.B. Brand, Tunneleinsturz, etc.), so äussert sich dies dadurch, dass entsprechende Umweltsensoren anschlagen. Diese liegen aber ggf. recht weit auseinander und der Ort der Messung ist aufgrund der immer vorhandenen Bewetterung (Luftströmung) nicht der Ort des Entstehens. Da die Abstände der Netzknoten untereinander
25 wesentlich geringer sein können als die Sensorabstände – und da bei LWL-Leitungen ja unter Umständen auch eine direkte Messung des Abstandes zu einer Unterbrechung erfolgen kann, ergibt sich über den Ausfall einer Netzwerkverbindung zusammen mit den im Abwetterstrom liegenden Sensorinformationen eine recht genaue Lokalisierungsmöglichkeit, welche für zwei Zwecke verwendet werden kann: a.) auf der Zentraleseite für die Einleitung von
30 Grubenwehraktionen (Rettungskräfte); b.) untertage für die Information der Belegschaft und die Erzeugung von dynamischen Evakuierungs- und Verhaltenshinweisen durch die Netzknoten.

Aktive Netzwerkkomponenten wie Switches und Accesspoints erfüllen normalerweise nur passive Netzwerkfunktionen, d.h. sie sind nicht aktiver Bestandteil irgendwelcher

Anwendungen. Die Erfindung basiert auf der Tatsache, dass in jeder aktiven Netzwerkkomponente eine Kontrolleinheit, z.B. als ein zusätzlicher Computer, eingebaut oder lokal zugeordnet ist (oder es wird eine der bereits im Switch oder Accesspoint vorhandenen CPU's genutzt), der das Gerät zu einem aktiven Bestandteil der Anwendungen speziell in sicherheitlicher Hinsicht macht. Daneben können von diesem „Netzwerkrechner“ auch andere Anwendungsfunktionen mit übernommen werden (wie z.B. das Verfolgen von Maschinen oder Personen).

Das Verfahren besteht aus den folgenden Verfahrensabschnitten:

- 10 1. Normalbetrieb (es liegt kein Notfall vor)
2. Notfall mit oder ohne Netzwerkverbindung zu Zentralsystemen – Selbstrettungshilfe sowie zentrale Einleitung von Rettungsmassnahmen
3. Netzwerkbasierte Notfallunterstützung von Rettungsaktionen.

Dies geschieht durch Teilfunktionen des Gesamtverfahrens, welche einzeln oder in Kombination eingesetzt werden können:

Für den Fachmann ist klar, dass der genannte zweite Punkt der Einleitung von Rettungsmassnahmen sowohl von Grubenseite als auch von zentraler Seite ausserhalb des Bergwerks kommen kann. Zudem können beide Seiten um die möglicherweise noch bestehenden Verbindungen und somit koordinierbaren Massnahmen „hinter“ einem Unfallpunkt, also einem Unterbruch, wissen.

Netzwerkredundanz durch Ringe und Meshing:

Im Normalmodus und im Notfallmodus sind die Netze so aufgebaut, dass eine Ringredundanz entsteht. Wird ein Ring allerdings an zwei Stellen unterbrochen, so entsteht u.U. eine Insel, die nicht mehr erreicht werden kann.

Durch eine wahlfreie Verbindung von Geräten untereinander kann die Ringredundanz zusätzlich durch „Querverbindungen“ ähnlich eines Spinnennetzes („mesh“) weiter abgesichert werden. Damit kann eine Netzwerkinfrastruktur aufgebaut werden, die genau dem Aufbau eines Tunnelsystems, Bergwerkes oder grossen Gebäudekomplexes entspricht:

Voraussetzung dazu ist lediglich, dass in jedem Tunnel (oder Flur) eine drahtgebundene oder drahtlose Netzwerkverbindung zwischen zwei aktiven Netzknoten möglich ist.

Damit ist das Netz in der Lage, für die Aufrechterhaltung der Kommunikation immer selbst nach alternativen Wegen zu suchen, sollte eine Verbindung ausfallen („selbsteheilendes Netzwerk“).

- 5 Es entsteht damit auch automatisch ein Abbild der physikalischen Struktur des (untertage-) Gebäudes über den momentanen Status aller Netzwerkverbindungen.

Lokales Einspeisen von Umweltdaten:

- 10 Im Gesamtverfahren werden sicherheitsrelevante Informationen wie Daten der Gassensoren oder die Wettersensorik (Luftgeschwindigkeit, Temperaturen etc) direkt am Ort des Entstehens in das lokale Netz eingespeist. Dies kann über Direktanschluss der Sensoren am Netzwerkrechner, über Sensornetze, über separate netzwerkfähige Anschlussgeräte oder über den Anschluss eines örtlichen Wetterrechners erfolgen.

- 15 Die Daten der Sensorik sind für den nächstgelegenen Netzwerkrechner zugänglich. Dieser führt ggf. auch die Vorverarbeitung der Daten durch und/oder transformiert diese in menschenlesbare Informationen (Umrechnung von Digitalwerten in SI-Einheiten etc.).

Im Normalbetrieb gibt der Netzwerkrechner die Informationen an „übertägige“ Zentralsysteme weiter.

20

Im Notfallbetrieb stellt jeder Netzwerkrechner innerhalb einer Insel die ihm zugeordneten Sensorinformationen allen anderen Netzwerkrechnern und ggf. angeschlossenen Netzwerkclients über das Netzwerk lokal zur Verfügung.

25 Überblick über den Netzwerkstatus und Selbstüberwachung:

- Jeder aktive Netzwerkrechner hat idealerweise einen vollen Überblick über die Gesamtstruktur des Netzes oder zumindest in seinem lokalen Einzugsbereich, und verfügt damit selbst oder in Koordination mit seinen Nachbarn über den Netzwerkstatus bis zu allen relevanten Notausgängen und / oder Rettungsmitteln (Rettungskabinen - „shelter“ etc). Diese Statusinformationen über die aktiven und verfügbaren bzw. nicht verfügbaren Netzwerkverbindungen werden im Normalbetrieb und im Notfallmodus permanent zwischen den Netzwerkrechnern ausgetauscht. Unter dem Begriff voller Überblick ist vorteilhafterweise verstanden, dass die tatsächliche örtliche Lage und die Verknüpfungen aller einzelnen Rechner präsent ist und dass diese Daten miteinander verknüpft sind. Das kann eine Datenbank sein,
- 30

deren Inhalte für menschliche Betrachter nachvollziehbar auf einem Display darstellbar sind. „Alle einzelne Rechner“ bedeutet hier logisch verknüpfte „lokale Rechner“, was bedeutet, Rechner, die zu einem verbundenen Schachtkomplex gehören, also Netzwerkrechner, über deren physikalischen Ort eventuell ein Notfallweg körperlich führen könnte. Die Informationen in einem solchen Überblick können regelmässig aufgefrischte Sicherheitsinformationen sein, 5 Informationen zu Standorten von Notausgängen, Rettungskammern etc., die im Notfallmodus prioritär und gegebenenfalls automatisch im Wechsel angezeigt werden.

Dabei überwacht z.B. jeder Netzwerkrechner permanent die logischen oder physikalischen 10 Verbindungen zu seinen „Nachbarn“. Dies kann durch rein logische Techniken und Kontrolltelegramme auf IP-Ebene erfolgen wie auch durch Abfragen des Linkstatus über den im Netzwerkrechner eingebauten oder an den Netzwerkrechner angeschlossenen Switch. Diese Abfragen erfolgen dann vorzugsweise über standardisierte Verfahren wie z.B. SNMP. Die Stati werden im Normalbetrieb an die Zentrale und/oder an die erreichbaren Netzwerkrechner 15 gemeldet. Dies kann z.B. über Broadcast-Telegramme erfolgen. Das Ausbleiben der Meldung von einem Netzwerkrechner führt dann zu einem Fehlerstatus und das System schaltet die Netzwerkwege ggf. auf eine Alternativstrecke um (siehe oben.).

In diesen Statusmeldungen können auch die dem Netzwerkrechner zugeordneten Umweltdaten 20 sowie Informationen über das Gerät selbst (wie z.B. der Batteriestatus) enthalten sein. Damit entsteht eine Selbstüberwachung des Netzwerkes welche im Notfallmodus von grosser Bedeutung ist. Auch im Normalbetrieb ist diese z.B. für die Wartung und Instandhaltung des Netzwerkes wichtig.

25 Jeder Netzwerkrechner verfügt auch über die entsprechenden Informationen über Rettungswege und Sicherheitsausrüstung, welche z.B. beim Bootvorgang von einem zentralen Server geladen und dann permanent im Netzwerkrechner gespeichert und bei Änderungen aktualisiert werden, sodass diese im Notfall in aktueller Form zugänglich sind, auch wenn die Verbindung zum entsprechenden Zentralsystem („Server“) unterbrochen ist. Mit diesen im Netzwerkrechner 30 vorhandenen Informationen werden wichtige Funktionen für die Evakuierung und das richtige Handeln in einem Notfall für die Personen im Notfallbereich verfügbar. Diese werden in den folgenden Abschnitten beschrieben:

Aufspaltung der Netzwerke im Notfallmodus:

In einem Notfall kann davon ausgegangen werden, dass die Verbindung des Untertagenetzwerkes zu den zentralen Einrichtungen z.B. über Tage oder in einer Steuerzentrale unterbrochen wird, selbst wenn diese redundant ausgeführt ist. In einem solchen Fall entstehen
5 eine – oder auch mehrere – Netzwerkinseln, welche dann ganz oder teilweise funktionsfähig bleiben. Eine solche Insel kann aus einem oder mehreren aktiven Netzwerkrechnern bestehen.

Der Notfallmodus wird von den aktiven Netzwerkrechnern in der (oder den) noch funktionsfähigen Inseln dadurch erkannt, dass keine Verbindung zu den Zentralsystemen mehr
10 besteht.

In diesem Fall schalten sich die Netzwerkrechner in einen Notfallmodus, in dem sie selbst in gewissen Zeitintervallen versuchen, Kontakt zu den nicht mehr vorhandenen „Nachbarn“ aufzubauen, um die Insel grösser werden zu lassen und ggf. erkennen zu können, wenn der
15 Kontakt zu den Zentralsystemen wiederhergestellt wird.

Im Notfallmodus übernimmt ein Netzwerkrechner in einer Insel die im Notfall wichtigen netzwerkadministrativen Funktionen des Zentralsystems wie z.B.:

- Vergabe der Netzwerkadressen an sicherheitsrelevante Geräte wie (Mobil-) Telefone,
20 sicherheitsgerichtete Sensorik u.ä. über einen im Notfallmodus zu aktivierenden DHCP-Server;
- Aktivierung eines SIP-Servers als Zentralgerät zum Aufbau von Sprachkommunikation innerhalb der „Insel“.

Welcher Netzwerkrechner diese administrativen Zusatzfunktionen übernimmt, wird unter den
25 Netzwerkrechnern z.B. über Zufallsprinzipien ausgehandelt: Dies kann z.B. dadurch geschehen, dass ein Netzwerkrechner, welcher den Ausfall als erstes erkennt, durch Aussenden eines Broadcast-Telegramms alle anderen in der Insel informiert, dass er selbst die netzwerkadministrativen Zentralfunktionen übernommen hat. Alternativ kann auch immer der Rechner im Zentrum der Insel die Zentralfunktionen übernehmen oder bestimmen, welcher
30 seiner Nachbarn welche Zentralfunktion zu übernehmen hat. Dabei wird derjenige Netzwerkrechner zum Master, welcher am weitesten von allen Endpunkten des Netzwerkes entfernt ist. Dies ist sicherheitstechnisch am sinnvollsten, da damit weitgehend ausgeschlossen werden kann, dass sich dieser Rechner nahe an einem Gefahrenpunkt befindet.

In die Berechnungen zur Bestimmung des Master-Rechners kann auch der Batteriestatus der Netzwerkrechner eingehen, sodass vermieden wird, dass ein Rechner mit einer geringen Batteriekapazität zum Master benannt wird. Alle anderen Rechner werden damit automatisch jeweils zu einem Slave.

5

Diese Verfahrensmerkmale beinhalten vorteilhafte Ausgestaltungen der Erfindung dahingehend, dass die Anzeige des jeweiligen lokalen Rechners den aktuellen günstigsten, für das Netzwerk erkennbaren Weg aus der Gefahrenlage anzeigt, wobei dies ein Weg nach draussen oder auch in einen Schutzraum oder einen als sicher eingestuften Raum des Untertagebereichs sein kann.

10

Werden zwei selbständige Inseln zusammengeschaltet (z.B. weil eine Verbindung zwischen zwei Inseln wiederhergestellt wird), so übernimmt der Netzwerkrechner derjenigen Insel mit der grösseren Anzahl aktiver Endgeräte („Clients“) die Zentralfunktionen für den neu geschaffenen grösseren Bereich. Das Zentralgerät in der ehemals kleineren Insel beendet seine

15

Erkennung der momentanen Lage in einem Notfall:

Durch die aktuellen Informationen über den Netzwerkstatus sowie die aktuellen Umweltinformationen kann jeder Netzwerkrechner innerhalb einer Insel auch ohne Verbindung zu einem Zentralsystem ein Bild über die komplette Sicherheitslage erhalten. Dies bezieht sich insbesondere auf die Lage von Notausgängen und den Weg dorthin sowie auf den Zustand der Wege zu den Notausgängen. Dabei wird eine bestehende Netzwerkverbindung vorzugsweise interpretiert als „Dieser Weg ist vermutlich für eine Evakuierung nutzbar“, wobei bestehende Umweltsensoren auf Gefahrenherde wie giftige Gaskonzentrationen oder Wassereintrich

25

Diese Informationen werden mit den im folgenden dargestellten Verfahrensschritten an die Personen weitergeben. Durch die ebenfalls auf den Netzwerkrechnern vorhandenen Grundinformationen über die Lokalisationen können damit auch Informationen z.B. über die Länge von Wegstrecken und die Position von weiteren Rettungsmitteln (Sauerstoff, Rettungsmasken, Tragen, Feuerlöscher etc) verfügbar gemacht werden. Insbesondere kann der Rechner aus den verfügbaren Informationen eine Sicherheitsinformation erstellen und auf einer Anzeige selbst optisch oder akustisch darstellen oder diese Sicherheitsinformationen über Netzwerk / WLAN an andere stationäre oder mobile Teilnehmer weitergeben.

30

Dynamische Evakuierungshilfe:

Liegen in allen Tunneln oder Fluren Netzwerkabel so kann über den im Netzwerkrechner vorhandenen Status auch erkannt werden, ob Rettungswege frei oder blockiert sind: Wenn ein
5 Netzwerkrechner erkennt, dass eine Verbindung zwischen zwei Netzwerkrechnern unterbrochen ist, so kann dies (ggf. unter Hinzuziehung weiterer Informationen wie z.B. *„Luftgeschwindigkeit in diesem Tunnel oder Flur ist gleich Null“* oder *„Lufttemperatur in diesem Bereich (an einem Netzwerkrechner) war oder ist sehr hoch“* so interpretiert werden, dass dieser Weg für eine Evakuierung von Personen nicht verfügbar ist. Diese Situation kann der Netzwerkrechner auch
10 ohne Verbindung zu Zentralgeräten an die Personen unter Tage oder im Gebäude weitergeben. Dies erfolgt vorzugsweise mit den folgenden Verfahrensschritten:

1. Eine Verarbeitungseinheit in einem Netzwerkrechner oder im Zentralsystem interpretiert die Werte der Umweltsensoren sowie die Stati der Verbindungen zu benachbarten Rechnern und erkennt z.B. das Über- / Unterschreiten von aus Tabellen oder Funktionen hervorgehenden sicherheitsrelevanten Schwellwerten. Daraus werden ein oder mehrere
15 Ausgangssignale abgeleitet, die auf Fluchtwege oder Fluchträume hinweisen und/oder die geeignet sind, solche Wege oder Räume auf angeschlossenen Anzeigeeinheiten zu visualisieren oder die auf die vermutliche Blockierung eines möglichen Fluchtweges (z.B. durch das Vorhandensein von sehr hohen Temperaturen und/oder CO-Messwerten)
20 hinweisen.
2. Die vermutliche Nichtverfügbarkeit des Fluchtweges wird unterstützt durch den zeitlichen Zusammenhang mit einem Abbruch der Netzwerkverbindung zu einem benachbarten Netzwerkrechner.
3. Die Verarbeitungseinheit generiert ein vordefiniertes Daten-Telegramm, welches alle
25 Teilnehmer im Netz erhalten und ggf. interpretieren können. Dieses Telegramm enthält mindestens die Positionsinformation der in die Verarbeitung eingehenden Sensor- und / oder Verbindungssignale und den entsprechenden Sensorwert und / oder die aus diesem Sensorwert zu ziehenden Konsequenzen wie: *„Vermutlich brennt es hier“* oder *„Dieser Weg ist für eine Evakuierung vermutlich nicht verfügbar“*
- 30 4. Die Verarbeitungseinheit sendet das Telegramm an alle Teilnehmer im Netz (per Broadcast-Message) oder nur an solche Teilnehmer, welche diese Mitteilungen explizit erhalten sollen.
5. Eine Verarbeitungseinheit in den Empfangsgeräten interpretiert die Telegramme und stellt sie auf einem Display dar oder schaltet Hinweisschilder oder Lichtsignale

entsprechend, sodass die Mitarbeiter in eine alternative Richtung geleitet werden können (siehe Beschreibungen unten wie z.B. Leuchtturmfunktion, Display oder mobile Endgeräte).

- 5 Besteht noch eine Verbindung zu den Zentralsystemen, so können natürlich auch entsprechende Verhaltensanweisungen dynamisch von den Zentralgeräten auf die Netzwerkrechner heruntergeladen werden. Diese Informationen können alle Netzwerkrechner in der entsprechenden Insel an die Personen weitergeben, welche sich in ihrer Reichweite befinden. Dies erfolgt z.B. über die in den folgenden Punkten dargestellten Verfahrensschritte:

10

Sicherstellung der vollständigen Evakuierung

Tragen alle Personen entsprechende Tags (Transponder) mit sich und sind die Netzwerkrechner mit den zugehörigen Lesegeräten ausgerüstet, so ist das Verfahren in der Lage, die vollständige Evakuierung eines Bereiches zu erkennen und damit sicherzustellen, dass sich keine Personen
15 mehr in dem Bereich „hinter“ einem Netzknoten befinden. Dieser Verfahrensschritt läuft in folgenden Stufen ab:

1. Im Normalbetrieb erkennt jeder Netzwerkrechner über das Transponder-Lesegerät oder über WLAN die Transponder in seiner Nähe.
2. Der Netzwerkrechner gibt diese Informationen an ein Zentralsystem weiter.
- 20 3. Gleichzeitig speichert der Netzwerkrechner die personenbezogenen Bewegungsinformationen mit Transponder-Nr und Zeitstempel über einen Zeitraum von mind. einer Schicht in einem eigenen eingebauten Speicher.
4. Ein Notfall tritt ein und die Verbindungen zum Zentralsystem gehen verloren.
5. Durch die nach 3. gespeicherten Bewegungsinformationen „wissen“ alle
25 Netzwerkrechner in einer Insel, welche Personen sich innerhalb der Insel befinden müssen:
 1. Personen, deren Transponder noch aktiv im Netz sichtbar sind
 2. Personen, deren Transponder nicht aktiv im Netz sichtbar sind, sich aber zum Zeitpunkt der Einleitung des Notfallmodus in einem nicht abgedeckten Bereich
30 zwischen zwei Netzwerkrechnern befunden haben: Diese wurden von einem oder mehreren Netzwerkrechnern erkannt und aufgrund der zeitlichen Reihenfolge der Leseereignisse kann ermittelt werden, dass sie sich noch im Bereich aufhalten. Dies gilt auch für Personen, die in einer „Sackgasse“ vom letzten Netzwerkrechner z.B. am Eingang der Strecke einmal erkannt, aber noch nicht ein zweites Mal beim Verlassen

festgestellt worden sind.

- 5
6. Ein Master-Rechner ermittelt den günstigsten Treffpunkt für alle im Bereich befindlichen Personen sodass diese entweder mit einer kürzestmöglichen Wegstrecke zum Versammlungspunkt („Muster Station“) kommen können oder sich an einem
- 10
7. Über die Netzwerkrechner werden die Personen (z.B. über die „Leuchtturmfunktion) oder Displays und dynamische Notfallschilder zum Versammlungspunkt geführt. Dabei sollten die Personen nur dann weitergehen, wenn die Netzwerkrechner ihnen (z.B. über wechselnde Farben der Leuchtturmfunktion) signalisieren, dass sich im Bereich „hinter“
- 15
8. ihnen keine Personen mehr aufhalten: Die Abwesenheit von schwarzen Pfeilen in Fig. 4 signalisiert personenfrie Bereiche in einer teilevakuieren Netzwerkinsel während sich bei den anderen schwarzen Pfeilen noch Personen „hinter“ den Netzwerkrechnern befinden. Der graue Pfeil zeigt den wahrscheinlichen besten Fluchtweg an.

Die Nutzung von Transponder-Information, die unter Umständen auf anderen Wellenlängen als die Netzwerkkommunikation stattfinden kann, gestattet eine Abbildung der

20

Evakuierungssituation und beinhaltet eine vorteilhafte Ausgestaltung der Erfindung.

Leuchtturmfunktion der aktiven Netzwerkkomponenten:

Eine blitzende LED an einem Netzwerkrechner signalisiert den Weg zu einem Rettungsmittel wie zu einer Rettungskabine oder zu einem offenen Notausgang. Dies kann sowohl für den

25

Normalbetrieb als auch für den Notfallbetrieb gelten. Diese „Leuchtturmfunktionen“ kann beispielsweise so ausgestaltet werden, dass die folgenden Mitteilungen anhand von farbigen Blitzen oder anhand von Blinksignalen übermittelt werden. Eine Farbcodierung könnte wie folgt aufgebaut sein:

Grün: Dieser Netzwerkrechner hat Verbindung zu einem Gerät, welches über

30

Netzwerkkontakt zu einem Notausgang oder einem Rettungsmittel verfügt;

Rot: Gefahr von gesundheitsgefährdenden Gasen im Reichweitenbereich des Netzwerkrechners;

Blau: Der Netzwerkrechner hat Verbindung zu einem Gerät, welches über Netzwerkkontakt zu einem Notausgang oder einem Rettungsmittel verfügt. Gleichzeitig herrscht Gasgefahr auf diesem Weg („Rettungsmasken benutzen“);

5 Weiss Keine Infos über Notausgänge oder Rettungsmittel verfügbar. Der Netzwerkrechner ist funktional.

Weitere Farbcodes oder Blinksignale können dazu dienen, personenfreie Bereiche anzuzeigen oder zu signalisieren, dass sich im Bereich „hinter“ dem Netzwerkrechner noch Personen befinden (s.o.).

10 Details über die jeweiligen Zustände können ggf. per Knopfdruck über ein Display (s.u.) oder drahtlos über PDA oder Mobiltelefone (s.u.) abgerufen werden.

Display für Notfall und Belegschaftsinformation:

15 Im Netzwerkrechner kann ein Display eingebaut (oder an diesen angeschlossen) sein, welches permanent oder nur auf Knopfdruck Sicherheitshinweise oder Belegschaftsinformationen darstellt. Derartige Informationen können z.B. sein: Dynamische Notausgangsinformationen: In Abhängigkeit von den Netzwerkinformationen über den Zustand von Fluchtwegen wird die Richtung eines Fluchtweges dynamisch angezeigt. Dies kann in Form eines Normsymbols für „Notausgang“ erfolgen. Dieser Normpfeil ändert dann in Abhängigkeit des aktuellen Zustands
20 der Fluchtwegen ggf. die Richtung und weist damit immer in Richtung eines vermutlich verfügbaren Notausganges und bietet damit einen wesentlichen Vorteil gegenüber den statischen Symbolen, welche immer nur statisch in Richtung des nächsten Notausganges zeigen können, obwohl dieser ja in Abhängigkeit der Lage blockiert sein könnte.

25 Das Display kann per Tastendruck aktiviert werden, um bei Batteriebetrieb im Notfall die Batterielebensdauer zu verlängern. Damit weist die LED (s.o.) den Weg zu einem Gerät und Detailinformationen sind per Knopfdruck über das Display verfügbar.

30 Auf dem Display kann dann auch die gesamte Lage z.B. in grafischer Form dargestellt werden, wobei die Wege zu Notausgängen sowie die Positionen von Notfallausrüstung in einer schematisierten Grafik oder in einem massstabgerechten 3D-Bild dargestellt werden können. Gleichfalls können per Tastendruck oder Touch-Screen z.B. Zusatzinformationen eingegeben und allen Personen bereitgestellt werden wie z.B. „der als blockiert angezeigte Notausgang ist

doch verfügbar (oder wurde von uns verfügbar gemacht) etc. Diese Informationen werden dann im Netzwerk verteilt und beeinflussen die Darstellung des Lagebildes. Dieses kann auch die Lokalisationen von Personen im Grubenbild beinhalten (s.o.)

5 **Informationsweitergabe an mobile Endgeräte:**

Da die Netzwerkrechner über WLAN-Accesspoints verfügen können oder Netzwerkkontakt zu solchen haben können, können in einem Notfall die relevanten Informationen auch für mobile Endgeräte zugänglich gemacht werden.

Dies kann mit den folgenden Verfahrensschritten geschehen:

- 10 1. Im Normalbetrieb erhalten die mobilen Endgeräte ihre Informationen z.B. über die Umweltdaten wie Werte von Gassensoren oder Informationen zur Luftgeschwindigkeit von zentralen Servern.
2. Da die Sensorinformationen lokal in das sicherheitsgerichtete Netz eingespeist werden, sind diese für den Nutzer von mobilen Endgeräten zugänglich.
- 15 3. Jeder Netzwerkrechner oder ein zentraler Netzwerkrechner in einer Insel stellt diese Informationen den mobilen Endgeräten zur Verfügung. Dies erfolgt z.B. über Web-Technologien wie Web-Browser oder JAVA-Anwendungen, per XML-Datagramme, per SMS – ähnliche Verfahren oder über speziell dafür definierte Datagramme.

20 **Lautsprecher-Funktionen der Netzwerkrechner und mobiler Endgeräte:**

Jeder Netzwerkrechner kann über eine Sprechstelle verfügen, welche aus Lautsprecher und Mikrofon sowie ggf. Zusatztasten besteht. Diese kann in den Netzwerkrechner eingebaut oder separat an diesen oder an das Netzwerk angeschlossen sein.

- 25 Im Normalbetrieb dienen diese Sprechstellen der Kommunikation mit der Belegschaft z.B. für allgemeine Durchsagen („PA“ = „Public Address“ System) zu Informationszwecken oder zur lokalen Warnung z.B. vor herannahenden Mobilmaschinen. Letztere können dabei auch automatisch vom Netzwerkrechner generiert werden, wenn z.B. eine Maschinen in den Drahtlosbereich eines Netzwerkrechners hinein fährt so warnt dieser und der nächste
- 30 Netzwerkrechner in der Kette vor der herannahenden Maschine über ein Tonsignal ähnlich einer Anfahrwarnung oder über eine automatisch abgespielte Sprachansage.

- Im Notfallbetrieb dienen die Sprechstellen zu Kommunikation der Personen, welche sich in einer Netzwerkinsel befinden oder mit einer Zentrale sofern noch eine Verbindung vorhanden ist. Dabei werden im Notfallmodus vorzugsweise alle Sprechstellen zu einer einzigen Gruppe
5 zusammenschaltet so dass alle Personen in der Insel sämtliche Gespräche mithören können. In diese Zusammenschaltung werden vorzugsweise auch die sprachkommunikationsfähigen mobilen Endgeräte sowie stationäre Telefone einbezogen so dass auch von diesen Geräten aus eine Kommunikation mit allen anderen Personen im Bereich möglich ist.
- 10 Die Zentralfunktionen der Sprachkommunikation („SIP-Server“) werden von dem zentralen Gerät übernommen, welches die administrativen Netzwerkfunktionen koordiniert oder von einem anderen Netzwerkrechner in einer Insel, falls keine Verbindung zu einem Zentralsystem (mehr) besteht.

15 **Energieabschaltungseinheit:**

- Im Falle von potentiell gefährlichen Gaskonzentrationen müssen – ggf. weit entfernt – Energieversorgungskomponenten abgeschaltet werden. Dazu können mit dem Netzwerkrechner Baugruppen verbunden sein, welche mit den Energieschaltgeräten über das Netzwerk in Verbindung stehen. Dabei werden die Umweltinformationen mitgenutzt, welche von der einem
20 Netzwerkrechner zugeordneten Sensorik ermittelt wurden.

- Die Erkennung der Sensorinformationen oder die Ableitung sicherheitskritischer und abschaltrelevanter Zustände kann vom Netzwerkrechner direkt per Software erfolgen, falls dies sicherheitlich zulässig ist. Andernfalls übernimmt eine externe Sensoreinheit diese Aufgabe und
25 der Netzwerkrechner stellt eine sicherheitsrelevante Kommunikation zur Abschalteinheit bereit.

- Die Abschalteinheit ist klassischerweise entweder mit einem (entfernten) Netzwerkrechner verbunden oder in diesen eingebaut oder direkt an einem Energieschaltgerät angebracht oder in dieses eingebaut.

- 30 Erkennungs- und Abschalteinheit stehen permanent in direktem Netzwerkkontakt miteinander und tauschen Telegramme über den Sicherheitsstatus aus. Diese Telegramme beinhalten Sequenz- und Zeitstempelinformationen wie auch Echtheitsinformationen. Ihre Inhalte sind vorzugsweise gegen Mißbrauch durch Verschlüsselung gesichert. Wird die Netzwerkverbindung

unterbrochen, so bleiben die Telegramme aus und es erfolgt aus Sicherheitsgründen eine sofortige Abschaltung. Gleiches erfolgt bei Inkonsistenzen in den Telegrammen oder wenn diese eine abschaltrelevante Sensorinformation signalisieren.

- 5 Die Energieabschaltung betrifft insbesondere Mittelspannungen zur Versorgung der Mine mit Energie im produktiven Einsatz. Die Netzwerkelemente, die gemäss der Erfindung eingesetzt werden oder durch das erfindungsgemässe Verfahren genutzt werden, sind einerseits mit gegenüber z.B. Funkenschlag geschützten Gehäusen versehen und verfügen entweder über eine auch batteriegestützte Spannungsversorgung für Notfälle.

10

Belegschaftswarnungen:

Ein Netzwerkrechner kann direkt oder über ein angeschlossenes oder im Netzwerk angeordnetes Peripheriegerät z.B. ausgelöst durch die Positionsinformationen von Menschen und Maschinen im Netzwerk audiovisuelle Warnungen auslösen, wenn sich z.B. Maschinen oder Fahrzeuge dem
15 Bereich nähern oder andere mögliche Gefahren über Sensoren oder über Datenmitteilungen aus dem Netzwerk erkannt werden. Derartige Datenmitteilungen können z.B. auch generiert werden, indem ein Mitarbeiter sich über bestimmte Telefonnummern in ein oder mehrere Geräte einwählt und eine Mitteilung selbst bekanntgibt oder damit das Abspielen einer vorbereiteten Mitteilung über Lautsprecheranlage und / oder Display auslöst. Dies kann auch z.B. über das Versenden von
20 Textmitteilungen geschehen, die manuell von Personen oder automatisch (z.B. von fahrenden Maschinen) generiert werden.

Unterstützung von Rettungsaktionen:

An jedem Netzwerkrechner oder an Zusatzgeräten innerhalb des Netzwerkes können optional
25 auch Rettungsausrüstungen angeschlossen werden, welche von Rettungsteams wie z.B. Feuerwehr oder Grubenwehr genutzt werden.

Damit werden diese Rettungsteams in die Lage versetzt, noch funktionierende Teile des Netzwerkes für ihre Arbeit mitnutzen zu können und eine bessere Kommunikation zwischen dem Rettungsteam vor Ort und der Einsatzleitung aufzubauen. Diese Kommunikation kann dann
30 z.B. auch Multimediainformationen von mobilen Kameras enthalten.

Zum Anschluss von Rettungsausrüstung dienen insbesondere die folgenden Funktionen:

1. Anschlüsse für Sprachkommunikationsgeräte;
2. Anschlüsse für traditionelle Rettungskommunikationssysteme;

3. Anschlüsse / Interfaces für Funkssysteme wie sie z.B. von Feuerwehr oder Polizei genutzt werden;
4. Anschlüsse für semimobile Netzwerkkomponenten zum Aufbau von temporären Netzwerken insbesondere für Rettungsteams.

5 **Anschlüsse für Sprach- und Rettungskommunikation:**

An den Sprechstellen oder Netzwerkrechnern können optional auch Anschlüsse für Sprechkombinationen vorhanden sein, welche z.B. in Rettungsmasken oder Vollschutzanzügen eingebaut sind. Dies ermöglicht auch eine Kommunikation wenn Personen unter Atemschutzbedingungen miteinander kommunizieren müssen sowie für Rettungsteams untereinander sowie wenn Rettungsteams versuchen, Kontakt zu anderen Personen in dem Bereich aufzubauen z.B. durch die Nutzung der Lautsprecherfunktionen.

Daneben können Anschlüsse für traditionelle Kommunikationsleitungen vorhanden sein, wie sie bereits heute von Rettungsteams z.B. in Bergwerken verwendet werden wie z.B. Prickerleitungen.

15

Anschlüsse für traditionelle Funkssysteme:

Im sicherheitsgerichteten Untertagenetzwerk können auch Schnittstellengeräte vorhanden sein, die die VoIP-basierte Sprachkommunikation des Netzwerkes mit dem Funksystem z.B. der Feuerwehr verbinden. Da die Reichweite der Funkgeräte unter Tage begrenzt ist, können sich damit die Rettungsteams auch über einen grösseren Bereich hinweg verständigen, weil Teile der Funkstrecke in digitaler Form über das Netzwerk (z.B. per VoIP) zurückgelegt werden. Andererseits ist eine direkte Kommunikation von den Rettungsfunkeinrichtungen mit Personen im Netzwerk z.B. über die Sprechstellen möglich. Diese Geräte werden entweder in einen Netzwerkrechner eingebaut oder an einer beliebigen Stelle im Netzwerk angeschlossen. Sie können permanent im Netzwerk installiert sein oder sie werden temporär während eines Einsatzes im Netzwerk angebracht.

25

Semimobile Netzwerkeinheiten für temporäre Einsätze und Rettungsteams:

Bei Rettungseinsätzen wird es vorkommen, dass diese in Bereichen stattfinden, in denen nicht mehr damit gerechnet werden kann, dass das Netzwerk funktionsfähig ist.

30

Gleichzeitig sind in den Netzwerkrechnern noch funktionsfähiger Netzwerkinseln Informationen gespeichert, die für ankommende Grubenrettungsteams wichtige Informationen enthalten können wie z.B. die Information, dass ein kompletter Bereich von Personen verlassen wurde, da keine Transponder mehr in diesem Bereich erkannt werden. Suchaktionen können sich somit vorrangig auf andere Bereiche konzentrieren. Um den Rettungsteams den Anschluss an untertägige Netzwerkinseln zu ermöglichen, temporäre Verbindungen zwischen Netzwerkinseln und einem funktionsfähigen externen Netzwerk wiederherzustellen sowie die Arbeit über eine permanente Netzwerkkommunikation zu erleichtern und sicherer zu gestalten und damit auch die Möglichkeit der Übertragung von Bild- und Videoinformationen vom Rettungsort an die Einsatzleitung zu ermöglichen werden mobile Einheiten eingesetzt, die von den Rettungsteams mitgenommen werden. Eine solche mobile Einheit besteht aus einer Kabeltrommel mit einem aufgerollten industriellen Lichtwellenleiterkabel oder mit einem kupferbasierten Netzwerkkabel (Fig. 4).

In den Kern der Trommel sind die Elektronik eines Netzwerkrechners sowie eines Accesspoints und eines Switches eingebaut. Ein Batteriepack kann entweder eingebaut sein und / oder mobil angeschlossen werden. Auch ist eine Stromversorgung über ein Hybridkabel möglich, in dem sowohl LWL als auch eine Versorgungsleitung enthalten sind.

Das Netzwerkkabel der Trommel wird an einem funktionsfähigen Switch oder einem Netzwerkrechner angeschlossen und ausgerollt.

Am Ende des Kabels wird die Kabeltrommel abgelegt oder aufgehängt. Stromversorgung und Antennen sowie ggf. weitere Peripheriegeräte werden an die Anschlüsse im Kern der Kabeltrommel angeschlossen. Durch den eingebauten Accesspoint ist in der Umgebung der Trommel auch eine Drahtloskommunikation möglich. Diese wird benötigt für z.B. drahtlose Sprachkommunikationsgeräte, drahtlose Sensoreinheiten für Umweltmessungen, Kameras oder Geräte welche die Vitaldaten der Personen des Rettungsteams überwachen und an die Einsatzleitung weitergeben um diese Personen nicht unnötig gesundheitlichen Gefahren aussetzen zu müssen.

Auch können im Kern der Kabeltrommel weitere Elektronikgeräte eingebaut werden, die für Rettungseinsätze hilfreich oder erforderlich sind wie z.B. Umweltmessgeräte oder Umsetzer für nicht-Ethernet basierte Funkgeräte. Die Verarbeitung der entsprechenden Daten kann dann von

der Verarbeitungseinheit des eingebauten Netzwerkrechners übernommen werden.

Die Kabeltrommel als Element eines Kommunikationsnetzwerkes kann auch in anderen provisorisch zu installierenden Netzwerken eingesetzt werden, wie auf provisorischen LAN's
5 oder wo mobile Kommunikation sich auf provisorische Mikrosender abstützen muss.

An die Netzwerkanschlüsse des Switches in jeder Kabeltrommel wird dann die nächste Kabeltrommel angeschlossen. Damit kann ein vollständig separates und mobiles Netz – auch über grössere Strecken - aufgebaut werden. Auch können die Trommeln dazu dienen, defekte
10 Netzwerkstrecken des fest installierten Netzwerkes vorübergehend wieder in Betrieb zu nehmen, um damit beispielsweise festzustellen ob sich in der damit neu angeschlossenen Insel noch Personen befinden.

Auch haben die Rettungsteams damit die Möglichkeit, über die Verbindung mit den stationären
15 Netzwerkrechnern abzufragen, welche Mobilgeräte sich im Bereich aktuell befinden oder welche sich in diesem Bereich befanden als der Notfallmodus eingeleitet wurde.

Initialisierung des Verfahrens:

Wird ein neuer intelligenter Netzwerkrechner in ein System einbezogen oder wird ein intelligenter Netzwerkrechner an eine andere Stelle im System „umgesetzt“ (relokalisiert), so
20 läuft ein automatisches Verfahren ab, in dem der Netzwerkrechner initialisiert wird. Dieser speichert alle Informationen in seinem eigenen Festwertspeicher ab, sodass diese auch nach einem Abbruch der Verbindung zu den Zentralsystemen weiterhin zur Verfügung stehen:

1. Erstinitialisierung an einem Ort, an dem bisher kein Gerät vorhanden war:
 - 1.1. Das Gerät meldet sich beim Zentralsystem an oder sucht aktiv nach einem solchen
25 oder es wird vom Zentralsystem selbsttätig gefunden.
 - 1.2. Ein Nutzer gibt auf dem Zentralsystem nach Autorisierung die Lokalität (Position) des Systems in den entsprechenden Grubenkoordinaten ein.
 - 1.3. Der Nutzer stellt ggf. weitere administrative Initialisierungswerte ein.
 - 1.4. Damit kennt das Gerät seine Position. Es verfährt nun wie für die Relokation des
30 Gerätes beschrieben (ab Schritt).

2. Relokation eines bereits erstinitialisierten Gerätes an eine andere Position:

2.1. Das Gerät meldet sich nach dem Einschalten und Anschluss des Netzwerkes beim Zentralsystem an

2.2. Das Zentralsystem stellt fest, dass anstelle eines früher an dieser logischen Stelle des Netzes befindlichen Gerätes eine andere Hardware installiert wurde.

2.3. Das Zentralsystem fragt einen Nutzer, ob das Gerät als direkter Ersatz an identischer Position wie das Altsystem installiert wurde. Wenn ja, dann wird sofort mit Schritt 4 weitergearbeitet. Wenn nein, dann erfolgt vor der Abarbeitung von Schritt 4 eine Bearbeitung der Schritte 2 und 3 aus der Erstinitialisierung.

2.4. Der Netzwerkrechner fragt seine „Nachbarn“ nach deren Positionen und den Verbindungen zu weiteren Geräte und baut sich damit sein eigenes Netzwerkmodell auf. Dieses wird in einem Festwertspeicher dauerhaft abgelegt. Alternativ können diese Informationen auch vom Zentralsystem auf den Netzwerkrechner heruntergeladen werden.

2.5. Das Zentralsystem lädt entweder die dazugehörigen Infrastrukturdaten (Länge der Netzwerkverbindungen und damit der Tunnelstreckenlängen) zwischen den Netzwerkrechnern auf die Netzwerkrechner herunter. Diese verbinden die Informationen mit ihren logischen Netzwerkdaten und kennen damit die Entfernungen zwischen den einzelnen Netzwerkrechnern. Alternativ kann der Netzwerkrechner diese Daten auch beim Zentralsystem (oder bei einem bereits installierten „Nachbarn“ erfragen. Letzteres vermeidet unnötigen Datentransfer über das gesamte Netz.

2.6. Darüber hinaus werden die Positionen von Notausgängen und Rettungsausrüstung ebenfalls vom Zentralsystem oder vom Nachbarn heruntergeladen.

2.7. Weiterhin können auch spezielle Koordinaten- und positionsabhängige Anwendungen von zentralen Systemen heruntergeladen werden, welche dem Gerät spezielle Aufgaben zukommen lassen, die z.B. von der Position des Gerätes abhängig sind wie: Abspielen von bestimmten Textwarnungen über die Lautsprecheranlage bzw. Einschalten des Displays, wenn Menschen in der Nähe vorbeigehen oder wenn sich Fahrzeuge oder Maschinen nähern.

2.8. Das Gerät geht in den Normalbetrieb und kann die verfahrensgemässen Aufgaben erfüllen.

Die Systeme sind damit für ihre lokalen Aufgaben zur Unterstützung der Grubensicherheit vorbereitet. Alternativ kann die Konfiguration auch manuell z.B. über Webbrowser erfolgen

Sicherheits-Fahrtenschreiber:

- 5 Im Notfallmodus schreibt das Gerät alle sicherheitsrelevanten Daten in einen Fahrtenschreiber, welcher im Festwertspeicher angebracht ist. Damit können ggf. nachträglich Daten über das Verhalten von Personen und Maschinen, deren Positionen etc ausgelesen werden.

System:

- 10 Das System besteht aus einem Rechner, der angeschlossenen lokalen Peripherie und den Netzwerkverbindungen zwischen den lokalen Einheiten und Zentralsystemen.

Im Normalbetrieb stellt das Gesamtsystem eine in sich geschlossene Einheit dar, welche für sich genommen den Bergwerksbetrieb erleichtert und durch Vereinheitlichung der Kommunikation
15 die eingesetzten Ressourcen für Investition, Installation, Betrieb und Wartung optimiert. Gleichzeitig ist das System auf der Grundlage von Ethernet offen um die Ankopplung zukünftiger Geräte und Systeme zuzulassen.

Das Gesamtsystem besteht aus einer Anzahl von intelligenten Netzwerkrechnern unter Tage,
20 welche zusammen mit ihrer zugeordneten Peripherie das Kernstück der Funktionalität ausmachen. Diese implementieren das oben erläuterte Verfahren.

Die notwendige Peripherie kann direkt im Gerät eingebaut sein oder direkt über verschiedene Schnittstellen an das Gerät angeschlossen sein oder über das Netzwerk angeschlossen sein.
25

Wichtig für das Verfahren ist lediglich, dass die Netzwerkrechner unter Tage die lokale Verarbeitung der Informationen vornehmen, um diese im Normal- oder Notfallbetrieb an die Belegschaft weitergeben zu können. Dabei spielt es keine Rolle, ob eine Netzwerkverbindung zu den Zentralsystemen vorhanden ist oder nicht.
30

Weitere Ausführungsbeispiele sind in den abhängigen Ansprüchen beschrieben.

KURZE BESCHREIBUNG DER ZEICHNUNGEN

Bevorzugte Ausführungsformen der Erfindung werden im Folgenden anhand der Zeichnungen beschrieben, die lediglich zur Erläuterung dienen und nicht einschränkend auszulegen sind. In den Zeichnungen zeigen:

- 5 Fig. 1 A & B eine schematische Darstellung eines Ringnetz bei Normalbetrieb und im Störfall;
- Fig. 2 A & B eine schematische Darstellung eines vermaschten Ringnetz bei Normalbetrieb und im Störfall;
- 10 Fig. 3 eine schematische Darstellung eines durch Netzwerkunterbrechungen abgeschnittenes Grubengebiet mit symbolischen Anzeigen an den Netzwerkrechnern (Pfeile) zur dynamischen Evakuierung und zur Anzeige, ob Teilgebiete evakuiert sind oder nicht; und
- Fig. 4 eine schematische Darstellung von der Seite einer Kabeltrommel mit einem im Kern der Kabeltrommel mit LWL oder Hybridkabel eingebauten Netzknoten mit
- 15 LWL-Anschlüssen und Funkzugang, Stromversorgung und zusätzlichen Peripherieanschlüssen 4) zur temporären Verbindung von Netzen durch Rettungskräfte oder zum Aufbau von selbständigen temporären Netzen für Rettungsaktionen.

20

BESCHREIBUNG BEVORZUGTER AUSFÜHRUNGSFORMEN

Die Fig. 1A zeigt ein Beispiel eines Netzwerkes in einer schematischen Darstellung als Ringnetz bei Normalbetrieb und im Störfall.

Der Switch 10 ist als Symbolbild für die ausserhalb der Untertageanlage angeordnete Netzwerkarchitektur dargestellt. Es bestehen zwei unabhängige Untertageringe 11 und 12, die über eine Ringstruktur verfügen. Jeder Ring verfügt hier beispielsweise über acht

30 Netzwerkeinheiten A1 bis A8 bzw. B1 bis B8, die generisch als Rechner 20 bezeichnet sind. Natürlich kann diese Zahl grösser und kleiner sind und die Verbindungen 21 zwischen zwei Einheiten können im Abstand mehrere 100 Meter Tunnellänge oder wenige Meter sein. Die Verbindungen 21 können auch Funkstrecken sein. Jeder Rechner 20 kann Sensoren zur Aufnahme von Umweltdaten wie Temperatur, Gaskonzentrationen etc. umfassen. Rechner

können unübersehbare äussere Anzeigeelemente zur Aussendung von optischen Warnungen und entsprechende Lautsprecher haben. Es können Schnittstellen (Kabel oder z.B. Bluetooth) zu Sensoren existieren und zu externen Headsets. Ferner sind Netzwerkschnittstellen vorgesehen und eine Eingabeeinheit wie eine Tastatur und eine Anzeige, insbesondere zur Anzeige von
5 Informationen betreffend zum Beispiel die Standorte von Rettungsmitteln, den Stand der dynamischen Evakuierung und Bereichsfreimeldungen (siehe Beschreibung zu Fig. 3), etc. .

Die Fig. 1B zeigt nun einen Störfall, wo an mehreren Stellen 22 die Verbindungen 21 aufgebrochen oder zerstört sind. Damit werden die schraffiert dargestellten Rechner 23 isoliert
10 und sind mit dem Rest des Netzwerkes nicht mehr verbunden. Man kann sie als Inselrechner 23 bezeichnen. Diese bilden Inseln 31 und 32. Die Rechner in 23 treten dann in einen Notfallmodus ein, wobei einer der Rechner jeder Insel A3 bis A6 bzw. B4 und B5 einen Masterstatus entsprechend der Beschreibung annimmt.

Die Fig. 2A zeigt einen Ring gemäss Fig. 1A mit drahtgebundenen oder drahtlosen Querverbindungen 41, 42, die gemäss grubentechnischen Gesichtspunkten angeordnet werden. Beim Eintreten eines Störfalles wie nach Fig. 1B werden die Verbindungen 42 aktiviert, während die Verbindungen 42 noch optional unverbunden bleiben. Das Suchen der (entweder drahtlosen oder drahtgebundenen) Verbindungen 41, was den Wiederanschluss der Rechner der Inseln 31
20 und 32 gestattet, ist eine der Funktionen der Inseln im Notfallbetrieb und der jeweiligen Masterrechner.

Alle gleichen oder ähnlichen Merkmale sind in allen Zeichnungen mit den gleichen Bezugszeichen versehen.

25 Die einzelnen Netzwerkrechner sind vorzugsweise in Ringen oder in vermaschten Ringen miteinander verbunden, um eine grösstmögliche Kommunikationssicherheit zu gewährleisten. Idealerweise liegt dabei in jedem Tunnelabschnitt ein Netzwirkkabel, womit dann ein ganzes Bergwerk logisch abgedeckt ist und die Netzwerkredundanz exakt der Redundanz der
30 Fluchtwege in einem Bergwerk entspricht.

Damit wird der Nachteil des konventionellen Ringnetzes vermieden, bei dem nicht erreichbare Inseln entstehen, sobald zwei Verbindungen oder aktive Komponenten ausfallen.

Werden diese Ringe untereinander vermascht, so bleiben die sonst abgeschnittenen Inseln mit einer viel höheren Wahrscheinlichkeit erreichbar.

5 Diese Umschaltungen werden von den Netzwerkrechnern automatisch im Bedarfsfall vorgenommen. Nicht aktive Netzwerkleitungen werden permanent von den beiden angeschlossenen Netzwerkrechnern überwacht.

Das Kommunikationswerk in einem Untertage-System umfasst ein untertage angeordnetes Ringnetzwerk von einzelnen Netzwerkrechnern. Mindestens einer, vorzugsweise mehrere
10 Netzwerkrechner sind über verschiedene Leitungen mit einer übertägigen Zentralsystemrechnereinheit verbunden. Unter Leitung wird dabei eine kabelbasierte Ethernetleitung, eine entsprechende Koaxialleitung, eine Lichtwellenleiterleitung oder kabellose Funkstrecken (WiFi, WLAN) verstanden. Jeder Rechner hat dabei einen Überblick über die Gesamtstruktur des Ringnetzwerks und einen zugewiesenen Netzwerkstatus. Unter Überblick
15 über die Gesamtstruktur wird die Netzstruktur nach Fig. 3 verstanden wie auch die Infrastruktur der Untertagestruktur selber, wie die Verteilung von sicherheitsrelevanten Orten und Gegenständen wie Notfallräume, Feuerlöscher, Notausgangsinformationen etc. Dazu gehören auch Raumklimadaten wie Abfragemöglichkeiten oder Darstellungsmöglichkeiten von Temperaturen, Gaskonzentrationen etc.. Der Netzwerkstatus entspricht den Möglichkeiten des
20 Geräts. Es kann in einer solchen Struktur wesentlichere Rechner und kleinere Rechneinheiten haben. Ein Teil der Statusinformation ist die veränderliche Statusinformation Normalbetrieb oder Notfallbetrieb. Unveränderliche Statusinformation ist die Information, ob der Rechner fähig ist, netzwerkadministrative Aufgaben zu übernehmen und ob er sie übernommen hat. Der Trigger für einen Wechsel des Status ist die Überschreitung eines Schwellwertes (wie beispielsweise
25 Gaskonzentrationsmesswerte eines Sensors; Temperaturmesswerte eines Sensors des Rechners) oder eines auslösenden Signals (Abbruch der Verbindung zu einem aus einer Gruppe von bestimmten anderen Netzwerkrechner; Eintreffen eines Notsignals von einem anderen Rechner des Netzwerkes oder eines mobilen Gerätes eines Mitarbeiters) etc. Neben der groben Abstufung Normalbetrieb und Notfallbetrieb können auch Zwischenstufen wie lokaler
30 Störfallbetrieb definiert sein.

Eine Vielzahl der Netzwerkrechner ist ausgestaltet, um im Falle eines Verbindungsunterbruchs zwischen Netzknoten zur Aufrechterhaltung der Kommunikation einen alternativen Kommunikationsweg zu suchen; alle müssen dazu nicht fähig sein.

- Eine Vielzahl der Netzwerkrechner ist mit mindestens einem Sensor versehen oder direkt oder über das Netzwerk verbunden, um die Umwelt betreffende Informationen aufzunehmen und ist ausgestaltet, um diese Information an andere Netzwerkrechner des Ringnetzwerkes und/oder an
- 5 das übertägige Zentralsystem weiterzugeben. Dies betrifft die besagten Temperaturen; Gaskonzentrationen; Luftbewegungen und Ventilationsinformationen etc., wobei die Netzwerkrechner im Normalbetrieb solche aktuelle die Umwelt betreffende Informationen an das übertägige Zentralsystem sowie an andere Netzwerkrechner weitergeben.
- 10 Wenn durch einen oder mehrere Unterbrüche die Netzwerkstruktur beschädigt ist; dann entstehen sogenannte Netzwerkinseln. Bei einer Vielzahl der Netzwerkrechner besteht die Möglichkeit, einen solchen Fehler festzustellen (=Verlust zum Routen von Information zum Zentralrechner übertage) und es wird dann in der durch einen oder mehrere Verbindungsunterbrüche solcherart entstandenen Netzwerkinsel der besagte Netzwerkstatus von
- 15 Normalbetrieb auf Notfallbetrieb gewechselt. Der Notfallbetrieb kann auch manuell durch einen autorisierten Benutzer oder – falls noch verbunden - z.B. vom Zentralsystem ausgelöst werden.
- Diese Rechner teilen dann auch diesen Status den nicht dafür ausgelegten Rechnern mit. Einer der besagten Netzwerkrechner mit dem Netzwerkstatus Notfallbetrieb nimmt dann einen
- 20 Masterstatus an und teilt allen anderen Netzwerkrechnern der Netzwerkinsel mit, dass sie einen Sklavenstatus annehmen sollen (Slave-Status). Für die Auswahl des Masterrechners können verschiedene Merkmale massgeblich sein. Es kann einer der schnelleren Rechner der Netzwerkinsel sein; der erste Rechner, der diesen Umstand feststellt; der zentrale Rechner im Knotenpunkt der gebildeten Insel; etc. Er ist auch ausgestaltet, um in der durch den
- 25 Verbindungsunterbruch entstandenen Netzwerkinsel netzwerkadministrative Funktionen des Zentralsystems zu übernehmen.
- Dieser Netzwerkrechner mit dem Masterstatus empfängt dann die besagten die Umwelt betreffenden Informationen im Notfallbetrieb und teilt diese allen anderen Netzwerkrechnern der
- 30 Netzwerkinsel mit. Alternativ ermitteln alle Rechner in der Netzwerkinsel den Status der ihnen zugeordneten Sensoren und teilen diese z.B. per Broadcast-Telegramm allen Netzwerkteilnehmern mit. Damit ist es dem mindestens einen Rechner möglich, im Zusammenspiel mit den in der Insel noch verfügbaren Informationen, dynamisch auf Schutzräume, Rettungswege; Gefahren aus Umweltbedingungen etc. hinzuweisen. Das kann

dann jeder Slaverechner. Zu den handelbaren Informationen gehören u.U. auch Telefonieverbindungen über Ethernetkabel (VOIP), einerseits als Telefoniebetrieb oder auch als Broadcast, damit alle betreffenden Personen in einer solchen Netzwerkinsel mit allen anderen Betroffenen, deren Nummer sie evtl. nicht kennen müssen, kommunizieren können; der Standort von Menschen und Material aus angemeldeten Handgeräten, der aufgezeichnet wird, so dass es später auslesbar ist.

Bei einer anderen vorteilhaften Ausgestaltung verarbeitet nicht nur der Masterrechner diese Umweltinformationen. Diese Verarbeitung kann auch verteilt durch die Rechner des Netzwerkes geschehen, an welche die Sensoren angeschlossen sind. Dies wird auch vorzugsweise der Fall sein, weil so auch kleinere Netzwerkinseln über den Vorteil der Zusammenführung und Verarbeitung der Umweltinformationen an einem Ort verfügen.

Eine weitere Funktion ist der Versuch der Selbstheilung des Netzwerks durch das Suchen nach alternativen Routingverbindungen 41, 42 zum Zentralrechner über Tage, wie es Fig. 2B darstellt. Es werden aktive Ping-Signale zum einen an die bekannten festen Adressen aber auch im Broadcast versandt, um mit mobilen Einheiten, die beispielsweise von Rettungskräften in das Untertagesystem eingebracht werden, in Verbindung zu treten, die dann die Verbindung mit dem Übertagenetzwerk herstellen.

Die Fig. 3 zeigt eine schematische Darstellung eines durch Netzwerkunterbrechungen abgeschnittenes Grubengebiet 50 mit symbolischen Anzeigen an den Netzwerkrechnern (Pfeile 51) zur dynamischen Evakuierung und zur Anzeige, ob Teilgebiete evakuiert sind oder nicht. Die Grube ist durch zwei Schächte 5 dargestellt. Übertage ist die Netzwerkanlage 6 durch ein Prinzipschaltbild dargestellt. Die Verbindungen 21 reichen durch die Schächte 5 in einen oder mehrere Stollen, von dem hier in Fig. 3 ein Prinzipschaltbild dargestellt ist. Letztendlich sind die Rechner 20 und die Verbindungen 21 unter Tage eine schematische Darstellung der Stollen einer bestimmten Sohle Vermaschungsverbindungen 41 und 42 können beispielsweise gerade eine Verbindung zwischen zwei Sohlen, also zwei Stollensystemen auf unterschiedlichem Tiefenniveau umfassen. Rechner 20 in einem Bereich 50 sind durch drei Unterbruchstellen 55, 56 und 57 vom Übertagenetz 6 abgeschnitten. Es entsteht eine Rechnerinsel 33 ohne Verbindung nach draussen.

Die Rechner 20 der Insel organisieren sich unter einem Masterrechner 29, für den verschiedene

hier genannte Kriterien möglichst kumulativ und nach Gewichtung zutreffen. Hier ist es ein Rechner 29 ausreichender Leistung mit genügender Batterieabsicherung in der Mitte der abgeschnittenen Insel. Durch Sensorinformationen von Rechnern 27 und 28 insbesondere zu Temperatur, Gas- und Staubkonzentration und gegebenenfalls vorbestimmten Parametern entscheidet der Masterrechner, dass der sinnvollste Rettungsweg in Richtung des Rechners 27 geht und ein Ausgang über die Abbruchstelle 57 am erfolgversprechendsten ist. Die Rechner 27 und 28 können in Bezug auf die bestehende Insel als Randrechner bezeichnet werden. Daher wird an allen Rechnern mit einer entsprechenden Anzeige ein Pfeilsymbol 51 gezeigt, in welche Richtung Bergarbeiter gehen sollen, die an einem der Rechner 20 mit einer entsprechenden Anzeige erscheinen. Gleichzeitig kann angezeigt werden, ob in einem Bereich „hinter“ dem Pfeil noch Personen mit einem Ortungsgerät / Transponder erfasst werden. Dies ist bei den „bereichsleeren“ Rechnern 26 nicht der Fall, so dass der Masterrechner 29 davon ausgeht, dass diese Grubenbereiche bereits menschenleer sind und somit nicht erste Priorität bei der Begehung durch Rettungskräfte haben. Der Weg der Pfeile 51 in Richtung Unterbruch 57 zeigt den am ehesten zu einer Evakuierung geeigneten Weg an.

Die Fig. 4 zeigt eine schematische Darstellung von der Seite einer Kabeltrommel 100 mit einem im Kern 101 der Kabeltrommel 100 mit LWL oder Hybridkabel eingebauten Netzknoten mit Lichtwellenleiter-(LWL)-Anschlüssen 103 und Funkzugang 102, Stromversorgung 107 und zusätzlichen Peripherieanschlüssen 104 zur temporären Verbindung von Netzen durch Rettungskräfte oder zum Aufbau von selbständigen temporären Netzen für Rettungsaktionen. Damit wird Rettungsteams der Anschluss an untertägige Netzwerkinseln 50 ermöglicht, da temporäre Verbindungen zwischen Netzwerkinseln 50 und einem funktionsfähigen externen Netzwerk 6 wiederhergestellt werden. Auf der Kabeltrommel 100 ist ein industrielles Lichtwellenleiterkabel 105 oder ein kupferbasiertes Netzkabel aufgerollt. Das eine Ende des Kabels 105 kann in einen mit dem Aussenrechner verbundenen Netzwerkrechner 20 eingesteckt werden, wonach dann die Benutzer der Kabeltrommel 100 diese entsprechend ihrem Vordringen ausrollen. Bei einem sinnvollen Einsatzpunkt oder am Ende der Kabelstrecke 105 wird die Trommel 100 hingelegt oder aufgestellt, zum Beispiel über ein Gestell an der Nabe 106, um weitere Komponenten anzuschliessen. Das andere Ende des Kabels 105 ist vorzugsweise schon von anbeginn mit einem entsprechenden innenseitigen Stecker/Buchse der Kabeltrommel verbunden oder angespleisst. Damit sind die Elemente 102, 103 und 104 direkt einsatzfähig, insbesondere, wenn eine Stromversorgung 107 angeschlossen ist. Alternativ kann in der Trommel 100 auch eine Spannungsversorgung integriert sein. An die LWL-Schnittstellen oder

Ethernetschnittstellen 103 kann dann die nächste Trommel 100 angeschlossen werden, oder, wenn eine Unterbruchstelle 57 überwunden ist, es kann die Netzwerkinsel 50 angeschlossen werden.

Im Kern 101 der Trommel 100 sind vorzugsweise auch die Elektronik eines Netzwerkrechners (sozusagen ein Rechner mit den Möglichkeiten eines Slaverechners 20) sowie eines Accesspoints und eines Switches eingebaut. Ein Batteriepack kann entweder eingebaut sein und / oder mobil angeschlossen werden. Auch ist eine Stromversorgung über ein Hybridkabel möglich, in dem sowohl LWL als auch eine Versorgungsleitung enthalten sind. Das Netzwerkkabel der Trommel wird an einem funktionsfähigen Switch oder einem Netzwerkrechner angeschlossen und ausgerollt. Die Trommel der Fig. 4 kann auch ohne den Einsatz eines Verfahrens gemäss Fig. 3 eingesetzt werden.

BEZUGSZEICHENLISTE

15

5	Schacht	51	Pfeilsymbol
6	Netzwerkanlage	55,56,57	Unterbruchstelle
10	Switch		
11,12	Untertagering	100	Kabeltrommel
20	Rechner	101	Kern
21	Verbindung	102	Funkzugang
22	Verbindungsunterbruch	103	LWL-Anschluss
23	Inselrechner	104	Peripherieanschluss
26	bereichsleerer Rechner	105	Lichtwellenleiterkabel
27, 28	Randrechner	106	Nabe
29	Masterrechner	107	Stromversorgung
31,32	Insel		
41,42	Querverbindung	A1-A8	Netzwerkrechner
50	Bereich	B1-B8	Netzwerkrechner

PATENTANSPRÜCHE

1. Kommunikationsnetzwerk in einem Untertage-Bauwerk (5), wobei an mehreren Knotenpunkten (20; A1-A8; B1-B8) untertägige Netzwerkrechner angeordnet sind, welche in einem Normalfall jeweils in einer Verbindung zu einer Zentralsystemrechnereinheit (6) stehen, wobei die Netzwerkrechner (20) ausgebildet sind, einen Notfall durch Verlust (22; 55, 56, 57) der Verbindung zu der Zentralsystemrechnereinheit (6) zu erkennen und dann einen Notfallmodus einzuleiten, **dadurch gekennzeichnet, dass** das Kommunikationsnetzwerk derart ausgebildet ist, dass im Notfall mindestens eine Netzwerk- oder Anwendungsfunktion der Zentralsystemrechnereinheit (6) von mindestens einem der untertägigen Netzwerkrechner (29) übernommen wird und dass mindestens eine Anwendungsfunktion (51) für den Notfall auf mindestens einem der untertägigen Netzwerkrechner (20, 26, 27, 28, 29) aktiviert wird.
2. Kommunikationsnetzwerk nach Anspruch 1, dadurch gekennzeichnet, dass jeder Netzwerkrechner (20) einen Überblick über eine Gesamtstruktur oder relevante Teile des Kommunikationsnetzwerks hat.
3. Kommunikationsnetzwerk nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass jeder Netzwerkrechner (20) einen zugewiesenen Netzwerkstatus aus einer Gruppe von vordefinierten Status hat; insbesondere Normalbetrieb und Notfallbetrieb
4. Kommunikationsnetzwerk nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass mindestens ein Netzwerkrechner (20; 29) ausgestaltet ist, um im Falle eines Verbindungsunterbruchs zwischen Netzknoten zur Aufrechterhaltung der Kommunikation einen alternativen Kommunikationsweg zu suchen.
5. Kommunikationsnetzwerk nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass mindestens ein Netzwerkrechner (20; 27; 28; 29) mit

mindestens einem Sensor versehen oder mit diesem direkt oder über eine separate Erfassungseinheit verbunden ist, um die Umwelt betreffende Informationen aufzunehmen, ggf. zu verarbeiten, insbesondere zur Auslösung eines Statuswechsels, und im Netzwerk weiterzugeben.

5

6. Kommunikationsnetzwerk nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass mindestens ein Netzwerkrechner (29) in einer durch einen Verbindungsunterbruch entstandenen Netzwerkinsel (31; 32; 50) ausgestaltet ist, im Notfallbetrieb einen Masterstatus als Netzwerkgerät der Netzwerkinsel (31; 32; 50) anzunehmen, wobei alle anderen Netzwerkrechner (20) der Netzwerkinsel
10 ausgestaltet sind, im Notfallbetrieb einen Sklavenstatus anzunehmen.

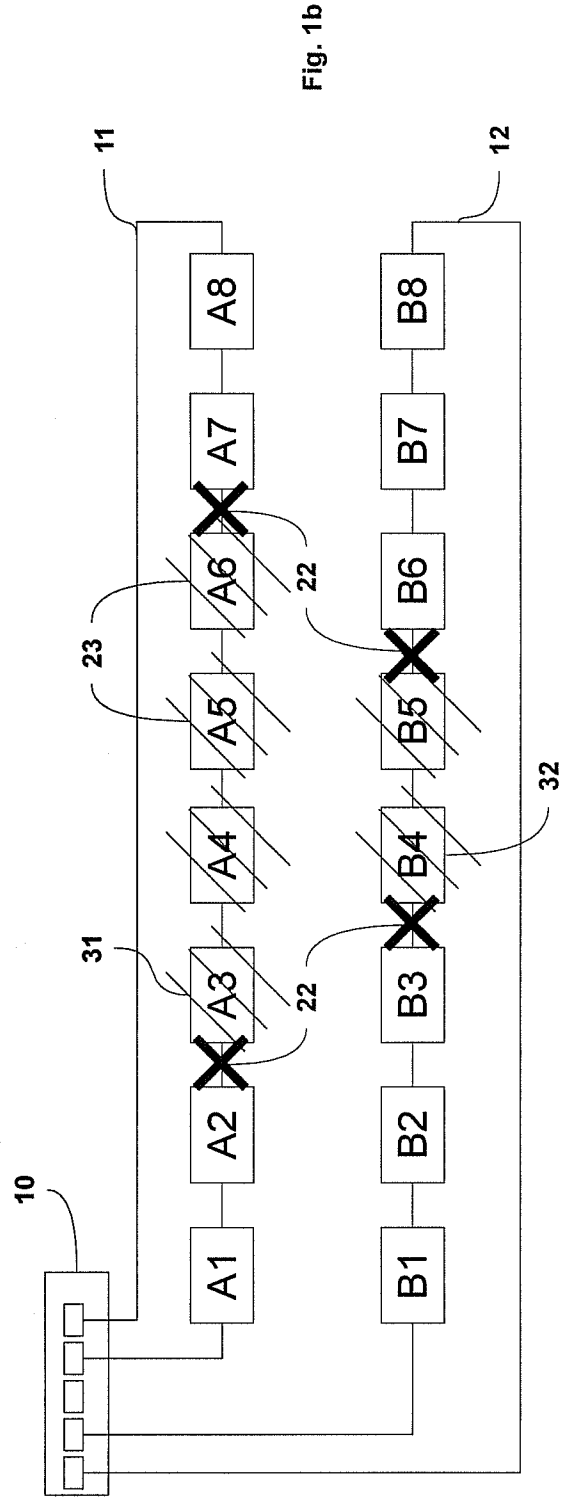
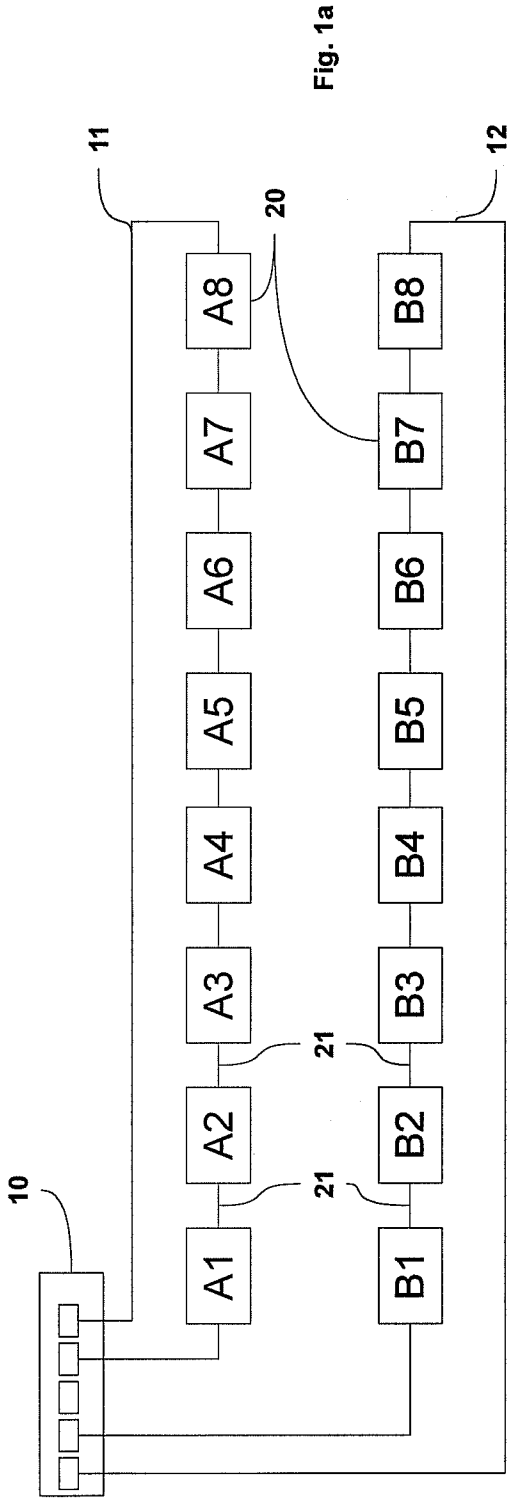
7. Kommunikationsnetzwerk nach Anspruch 6, dadurch gekennzeichnet, dass
15 mindestens ein Netzwerkrechner (29) ausgestaltet ist, die besagten die Umwelt betreffenden Informationen im Notfallbetrieb allen anderen Netzwerkrechnern der Netzwerkinsel zur Verfügung stellt und ausgestaltet ist. oder um in der durch den Verbindungsunterbruch entstandenen Netzwerkinsel Netzwerkfunktionen der Zentralsystemrechnereinheit (6) zu übernehmen.

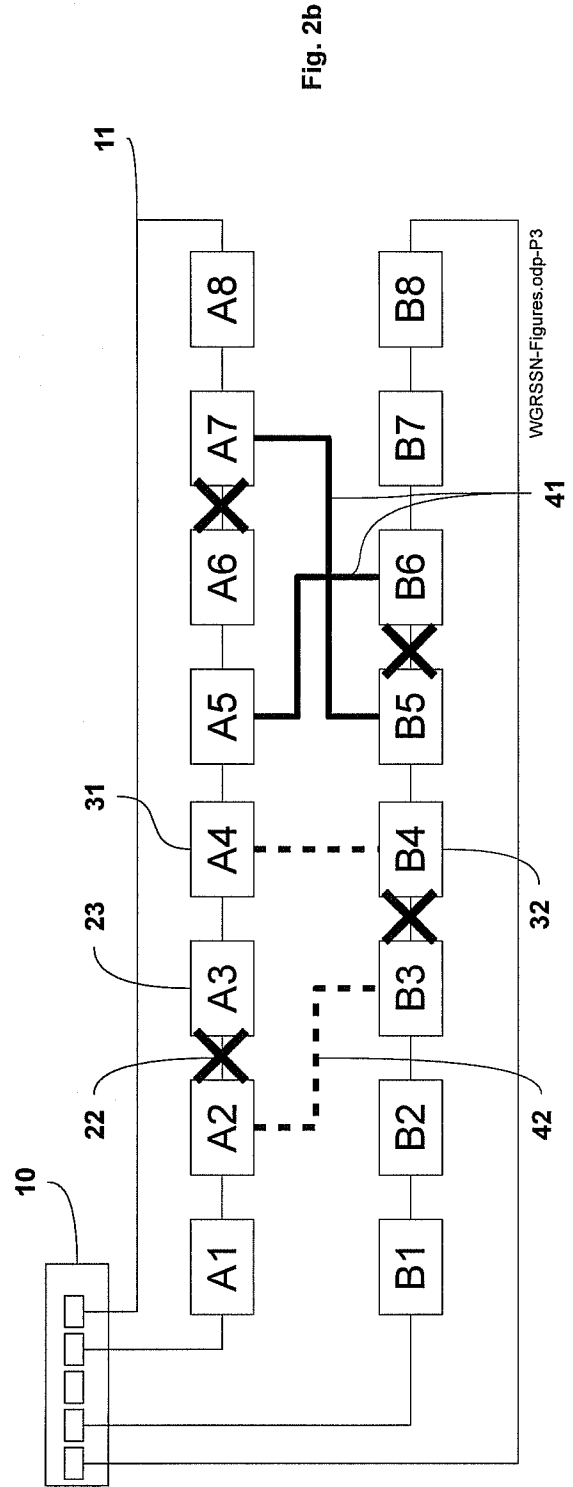
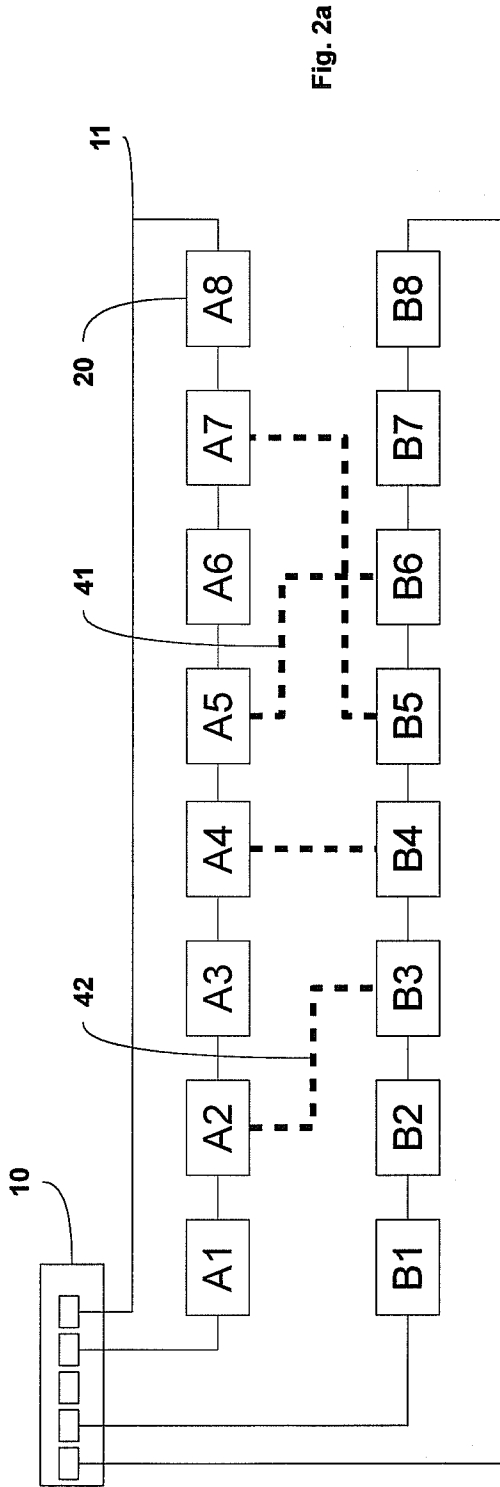
20 8. Kommunikationsnetzwerk nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass jeder Netzwerkrechner (20) innerhalb einer durch den Verbindungsunterbruch entstandenen Netzwerkinsel ausgestaltet ist, im Notfallbetrieb über einen Netzwerkstatus und aktuelle Umweltinformationen ein Bild über eine Sicherheitslage zu erstellen und auf einer Anzeige (51) optisch oder
25 akustisch darzustellen.

9. Verfahren zur sicherheitsgerichteten Kommunikation in einem Untertage-Bauwerk, wobei an mehreren Knotenpunkten angeordnete untertägige Netzwerkrechner in einem Kommunikationsnetzwerk bilden und bei einem Normalbetrieb jeweils in
30 einer Verbindung zu einer Zentralsystemrechnereinheit stehen, wobei mindestens ein Netzwerkrechner einen Notfall durch Verlust der Verbindung zu der Zentralsystemrechnereinheit erkennt und dann einen Notfallmodus einleitet, dadurch gekennzeichnet, dass mindestens ein Netzwerkrechner im Notfall

mindestens eine Netzwerkfunktion der Zentralsystemrechnereinheit übernimmt und dass mindestens eine Anwendungsfunktion für den Notfall auf mindestens einem der untertägigen Netzwerkrechner aktiviert wird.

- 5 10. Verfahren nach Anspruch 9, wobei der Notfallmodus auf der Basis von mindestens einer Sensorinformation und/oder Statusinformation oder manuell ausgelöst wird, insbesondere durch Abschneiden von einer vorbestimmten Anzahl von Netzwerkeinheiten von dem Übertagenetzwerk.
- 10 11. Kommunikationselement zum Aufbau von provisorischen Verbindungsstrukturen, insbesondere zum Einsatz mit einem Kommunikationsnetzwerk nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass ein Kommunikationskabel (105) auf einer Kabeltrommel (101) aufrollbar ist, wobei ein Ende des Kabels (105) mit der Kabeltrommel (101) verbunden ist, und wobei die Nabe und die Seitenelemente
- 15 der Kabeltrommel (101) über einen Anschluss für mindestens ein weiteres Kommunikationskabel (105) und eine inhärente Stromversorgung für eine in die Kabeltrommel (101) eingebaute Steuereinheit und Antenne einer drahtlosen Kommunikationseinheit verfügt.





WGRSSN-Figures.odp-P3

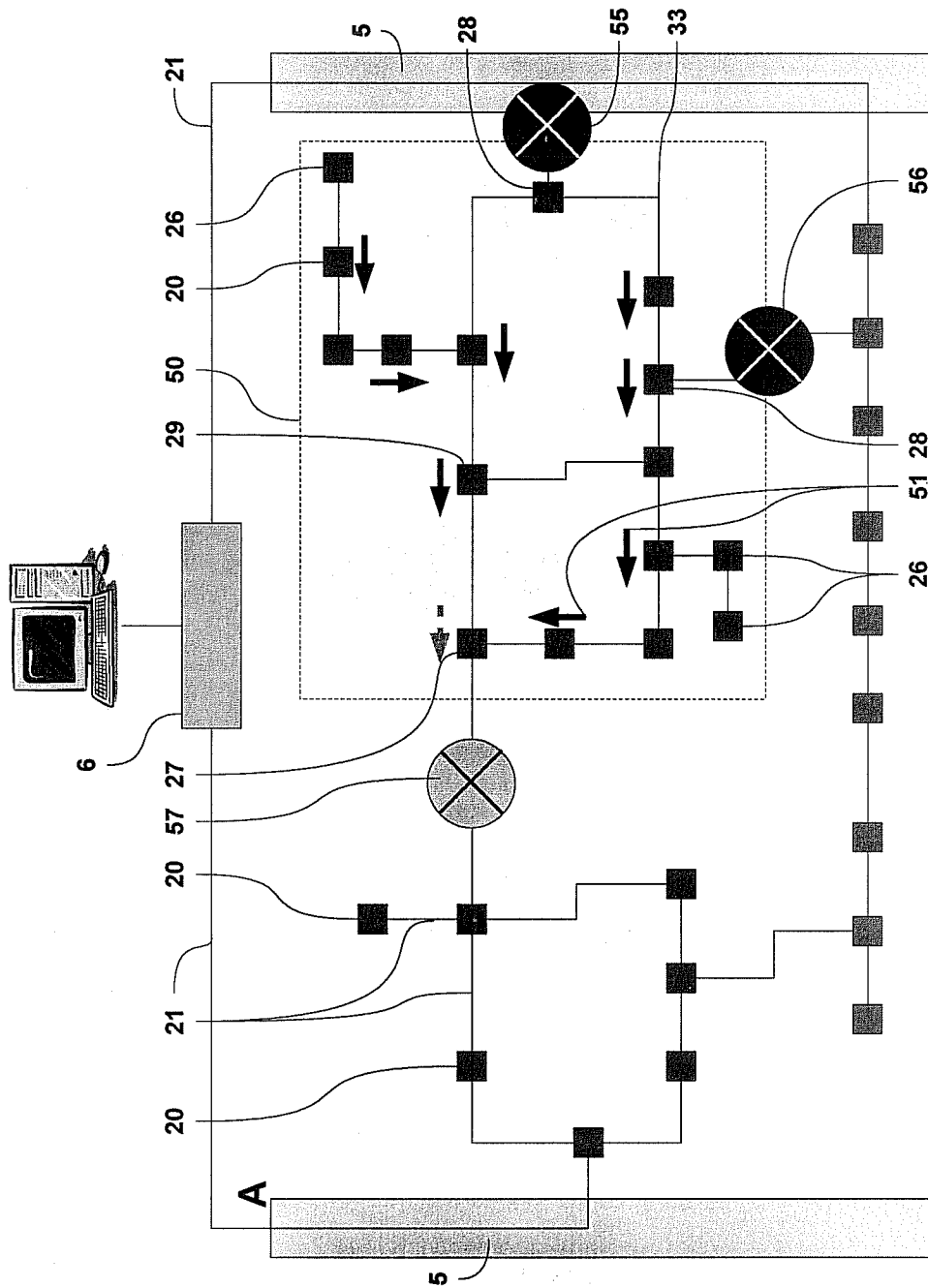


Fig. 3

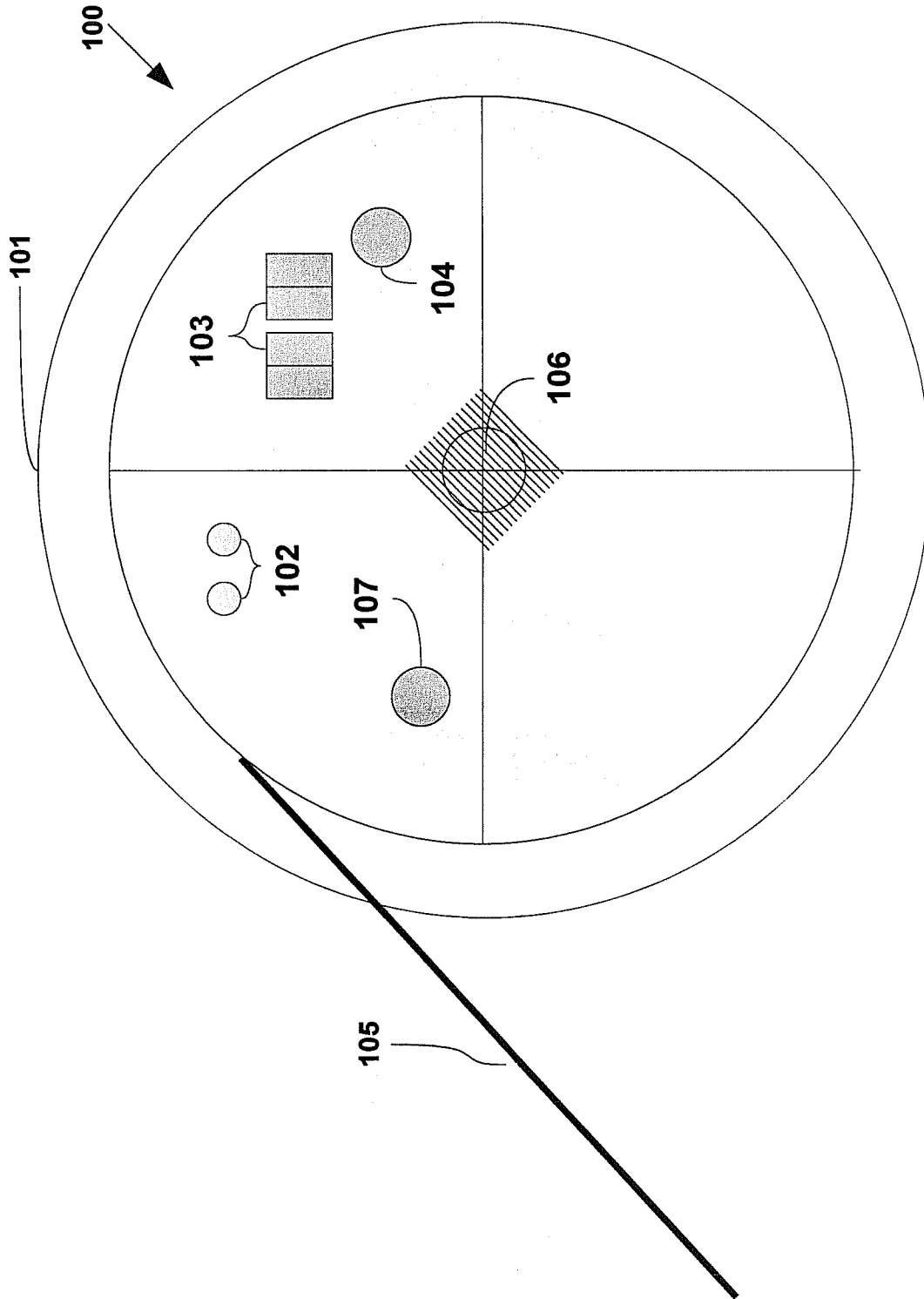


Fig. 4

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2010/056825

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04L12/437 H04L12/24
 ADD. H04L12/40

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Siemens: "OTN Produktbeschreibung. Ausgabe 11"[Online] 2006, pages 1-50, XP000863999 OTN Product Description (e-mail version) Retrieved from the Internet: URL:http://www.siptel.com/OTN/documents/description/german/S100_11_OTNdescription_GE.pdf> [retrieved on 2010-08-24] page 6 - page 8 page 16 - page 19 page 40 - page 41	1-11
X	WO 2008/065087 A2 (BECKHOFF AUTOMATION GMBH [DE]; BUETTNER HOLGER [DE]; WEBER KARL [DE]) 5 June 2008 (2008-06-05) page 2, line 15 - page 6, line 17 ----- -/--	1-11

 Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
 "E" earlier document but published on or after the international filing date
 "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
 "O" document referring to an oral disclosure, use, exhibition or other means
 "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

25 August 2010

Date of mailing of the international search report

22/09/2010

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040,
 Fax: (+31-70) 340-3016

Authorized officer

Kalabic, Faris

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2010/056825

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/207348 A1 (TSURUMI OSAMU [JP] ET AL) 22 September 2005 (2005-09-22) paragraph [0041] - paragraph [0083] paragraph [0136] - paragraph [0152] -----	1-11

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2010/056825

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2008065087 A2	05-06-2008	CN 101542981 A	23-09-2009
		DE 102006055889 B3	29-05-2008
		EP 2098018 A2	09-09-2009
		JP 2010510741 T	02-04-2010
		US 2009235001 A1	17-09-2009
US 2005207348 A1	22-09-2005	JP 2005269059 A	29-09-2005

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP2010/056825

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

INV. H04L12/437 H04L12/24
ADD. H04L12/40

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
H04L

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	Siemens: "OTN Produktbeschreibung. Ausgabe 11"[Online] 2006, Seiten 1-50, XP000863999 OTN Product Description (e-mail version) Gefunden im Internet: URL: http://www.siptel.com/OTN/documents/description/german/S100_11_OTNdescription_GE.pdf [gefunden am 2010-08-24] Seite 6 - Seite 8 Seite 16 - Seite 19 Seite 40 - Seite 41	1-11
X	WO 2008/065087 A2 (BECKHOFF AUTOMATION GMBH [DE]; BUETTNER HOLGER [DE]; WEBER KARL [DE]) 5. Juni 2008 (2008-06-05) Seite 2, Zeile 15 - Seite 6, Zeile 17 ----- -/--	1-11

Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen Siehe Anhang Patentfamilie

- * Besondere Kategorien von angegebenen Veröffentlichungen :
- "A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
 - "E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
 - "L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
 - "O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
 - "P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
 - "T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
 - "X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
 - "Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
 - "&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
25. August 2010	22/09/2010
Name und Postanschrift der Internationalen Recherchenbehörde Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Bevollmächtigter Bediensteter Kalabic, Faris

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2005/207348 A1 (TSURUMI OSAMU [JP] ET AL) 22. September 2005 (2005-09-22) Absatz [0041] - Absatz [0083] Absatz [0136] - Absatz [0152] -----	1-11

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2010/056825

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 2008065087 A2	05-06-2008	CN 101542981 A	23-09-2009
		DE 102006055889 B3	29-05-2008
		EP 2098018 A2	09-09-2009
		JP 2010510741 T	02-04-2010
		US 2009235001 A1	17-09-2009

US 2005207348 A1	22-09-2005	JP 2005269059 A	29-09-2005
