Universitatea *Transilvania* din Braşov
Şcoala Doctorală Interdisciplinară

Departamentul de Electronică şi calculatoare

Dipl. Ing. Christoph Müller

APPLICABILITY OF WIRED AND WIRELESS ETHERNET NETWORKING SYSTEMS AS UNIFIED SAFETY RELEVANT COMMUNICATION SYSTEM IN UNDERGROUND MINES

TEZĂ DE DOCTORAT

- PhD thesis -

Conducător ştiinţific:
Prof. univ. dr. ing. Iuliu SZEKELY

BRAŞOV

2013

Page intentionally left blank

0.1 Preface

In contrast to a conventional production factory or process plant which is operated in a static way after the plant has been built, an underground mine is a "*moving raw material factory*"[170], characterized by the fact that the factory itself (meaning the infrastructure of the mine with all its tunnels) permanently has to be developed and constructed under ongoing production. In addition, the special underground environment is characterized by a number of dangers and special conditions which increase the importance of communications[164] [156] [25].

Standard networking systems are more and more used as underground communication systems, however networking functions directly supporting mine safety are not yet used today. However if cables are available in most of the tunnels, the network forms an electronic representation of the underground infrastructure making it a the perfect carrier to implement safety relevant functionality like e.g. tracking people underground and guiding them to emergency exits[111][110][125]. Such functions supporting mine safety are critical in terms of:

- Mining specific legislation and rule-making
- General legislation and rule-making on occupational safety and health
- Survivability and functionality of the network components in terms of underground hazards or accidents

It is the goal of this thesis to demonstrate the feasibility of using Ethernet based networks as backbones even for safety relevant communication and to use extended network functionality to increase underground safety by having the network actively support the underground safety e.g. by helping to detect hazard locations by network interruptions and to actively guide people via the network to emergency exits and shelters.

The work related to thesis was performed in close conjunction with a research project about "*Emergency Support Technologies*" for mining co-funded by the European Commission's Research Fund for Coal and Steel ("*RFCS*") under the project No. RFCT2008-0001 and the project acronym "*EMTECH*". Parts of the testing and verification were performed within the RFCS project No. RFCP-CT-2011-00001 "*Demonstration of Process Optimization for Increasing the Efficiency and Safety by Integrating Leading Edge Electronic Information and Communication Technologies (ICT) in Coal Mines*" under the project acronym "*OPTIMINE*".

Page intentionally left blank

Table of Contents

Page intentionally left blank

Acknowledgments

"*Research and Development is not one man's sake*"*

Also the work for this thesis was carried out in several projects with major contribution of a number of individuals.

This includes all my staff at MineTronics GmbH in Ladbergen, Germany and MT-Silesia Sp.zo.o. in Wroclaw, Poland who were directly or indirectly taking part in the design and implementation of all the components of the system and for applying it in practice. They all helped and still are working with making the vision of a great new system become reality.

Special thanks to the Chief Systems Engineer at MineTronics, Dipl. Ing. György Biro for his mathematic and algorithmic creativity, for often hard-to-find simple solutions and for directing the details of systems implementation as well as to Andreas Hübner, M.Sc., for his Master Thesis in conjunction with the project and for taking care of all the deeply network related issues connected with development and systems application. Furthermore to Prof. Dr. Andreas Noack who was working with my companies during his B.Sc, M.Sc and PhD studies heavily involved into the project before he started his academic carrier at the FH Stralsund in 2011.

Special thanks also to RAG Anthrazit Ibbenbüren GmbH, especially to Dr. Max Stöttner, Michael Brenningmeyer and Jörg Bücker for the possibility and for their support to install the initial system components in their coal mine and for their flexibility in allowing to have the underground installations presented to visitors.

Last but not least very special thanks to all the people at the University of Transylvania in Brasov, especially to my mentor Professor Iuliu Szekely for their patience, their time and their professional support in making this thesis become reality.

- Cited from Karl Maas, AdB, as director of the R&D department at Heitkamp GmbH, my former principal.

Page intentionally left blank

Introduction

Underground mines are potentially dangerous working areas. Therefore, underground mine safety is traditionally regulated by related legislation. These rules also cover communication between the workers underground and above ground installations.

With the increasing demands on occupational health and safety and due to a number of major mining accidents involving people trapped underground it has been shown that conventional underground communication systems like telephones are not able to fulfill these demands any longer. In addition, mining companies today are obliged to fulfill the general legal obligations for safety and health of workers which also would require to meet related demands on functional safety and resilience of underground electronic communication systems.

Another operational fact today is that all safety relevant sensor information in a mine like ventilation speed, gas content in the air etc. is centrally processed above ground. Therefore it is not accessible to the people underground when the communication to above ground fails.

From this legal and operational basis research was required in two areas:

1. Creation of a standard based communication system with the highest possible hardware redundancy and resilience.
2. Making all vital environmental information accessible to the workers underground when no communication to above ground is available.

The necessity for this research was also respected by the European Commission's Research Fund for Coal and Steel (RFCS), which granted a related R&D project for Safety Support Technologies which these topics were part of. This project was carried out from 2008-2011.

From these two areas, this interdisciplinary thesis focuses on the basis of creating an Ethernet based wired and wireless underground communication system which has the capability of meeting functional safety standards (like Safety Integrity Levels "*SIL*") and which makes the network actively support the underground safety e.g. by keeping track of people's locations, by guiding people along the network to safe locations or to emergency exits and to advise about the underground environmental conditions on the evacuation routes. It thereby also forms the hardware and computational basis for the second research area which then can be implemented as applications running on the underground communication system hardware.

Structure of the Thesis

The thesis is divided into five main sections:

1. **Mining and Mine Communications** to explain basic knowledge from the underground mining industry and mine communications which is needed for readers who are not familiar with the mining industry in general and the special needs of underground mining communications in order to enable these readers to understand the details covered by the following sections. Readers with deep industrial knowledge and experience with Mine Communication Systems may skip this section for fast reading.
2. **Safety Support for Mine Communications**. This section explains the use and application of Ethernet based communication systems in underground mining and safety support functions and their relevance for future mining communication systems. This section mainly covers the general ideas developed during the work on this thesis.
3. **Implementation of the underground hardware.** This section explains the general implementation of the Ethernet based Mine Communication System explained in chapter 2 and focuses on the implementation details of the networking hardware in use underground consisting of the stationary network infrastructure hardware and the mobile application devices.
4. **Implementation of Central Servers and System Functionality.** This section explains the implementation of the central systems needed above ground and the functionality of the Safety Support System. After a description of the central server systems all general and system wide implementation of the functionality is explained. The essential Emergency Mode Detection functional implementation is described in detail before the implementation of the Emergency Mode handling and the related services are illustrated. Finally the realization of the recovery from Emergency mode is described

   Experience and Future Developments. This section contains statements about the operational experience with the parts of the system implemented and an outlook for the further upcoming development in the future.

1 MINING AND MINE COMMUNICATIONS

This section explains basic knowledge from the underground mining industry and mine communications which is needed for readers who are not familiar with the mining industry in general and the special needs of underground mining communications in order to enable these readers to understand the details in the following sections.

Readers with deep industrial knowledge and experience with Mine Communication Systems may skip this section for fast reading.

1.1 Underground Mining

This chapter covers a short description of mine safety in general and concentrates on the communication related issues of mine safety. It also covers a comparison with related rules for commercial tunneling installations.

"*Mining is the extraction of valuable minerals or other geological materials from the earth*"[172]. Mining happens mainly in two different extraction methods as open pit mining (surface mining) and underground mining (sub surface mining)[50][172]. All further developments described in this thesis refer to underground mining.

1.1.1 Underground Mining

Underground mining "*consists of digging tunnels or shafts into the earth to reach buried ore deposits. Ore, for processing, and waste rock, for disposal, are brought to the surface through the tunnels and shafts*" [172].

These shafts and tunnels are needed for any activity in an underground mine: They have to be used to supply material to the production areas as well as to the tunnel driving locations and for all personnel transport. Another purpose of shafts and tunnels in an underground mine is to assure that all underground areas are properly supplied with fresh air ("*mine ventilation*").

The geospatial layout of the tunnels follows certain rules basing on the needs of ventilation, transportation methods and machines used and personnel safety. The latter especially in relation to the number of emergency exits and their locations and distance from the workplaces[50][76][79].

Furthermore the tunnels and shafts also contain all supply lines for continuous supply of media like electricity, fresh water, liquified concrete etc[50].

Production is carried out in different methods depending on the raw material deposit and the kind of material to be extracted. These methods can be "*mechanical*" using large scale machinery or "*conventional*" using drilling and blasting techniques[50].

The transport of the extracted ore and also the transport of the waste rock is performed by either conveyor belt installations in the tunnels or by vehicles (loaders, trucks) or by trains[50]. Often also a combination of different methods is used[50].

Therefore, the tunnel layout of a mine is of crucial importance for any underground

mining operation.

1.1.2 Operation Management

In today's underground mining, many processes and machines are partly or fully automated with processes operated remotely controlled from above ground control rooms or operation centers [170][143][160].

This involves the use of electronic automation equipment like PLC's installed in the field and Supervisory Control And Data Acquisition ("SCADA") software systems for process control. So far, this is comparable to controlling a process plant [170][143][160].

In contrast to an above ground plant however, the structure of the mine changes while the plant (the mine) is in operation. Furthermore, unexpected works or events lead to tunnels which may not be used or are blocked which in turn results in the requirement of changing the operational routines.

Furthermore, a large amount of data like environmental and ventilation data, the locations of vehicles and people by nature are location dependent, which cannot be perfectly shown in a traditional SCADA system. The real time display of such information however is needed in order to enable a real time optimization of the ongoing underground operations[54].

For all this process optimization, the importance of network communication increases. As in industrial communication[37][57] above ground, the need for a permanent online availability of all process information is steadily growing as future productivity increase only can be achieved by a real time coordination of all ongoing process parts and a resulting reduction of expensive downtimes[112][160].

1.1.3 Geospatial data and location based mine supervision

The tunnel structures today are planned in CAD systems[84] and surveyed thoroughly with the survey results available in 2D or even 3D geospatial databases [54]. This means that a vectorized model of the mine layout in most cases is available in electronic form. A sample picture of a mine layout taken from a 3D modeling tool is shown in Figure 1.

When a real time 3D operation management software is used for mine operation, the current operating situation can be followed directly within the mine layout in a location based context[54]. This means, that the operator sees e.g. a train moving through the mine as well as he

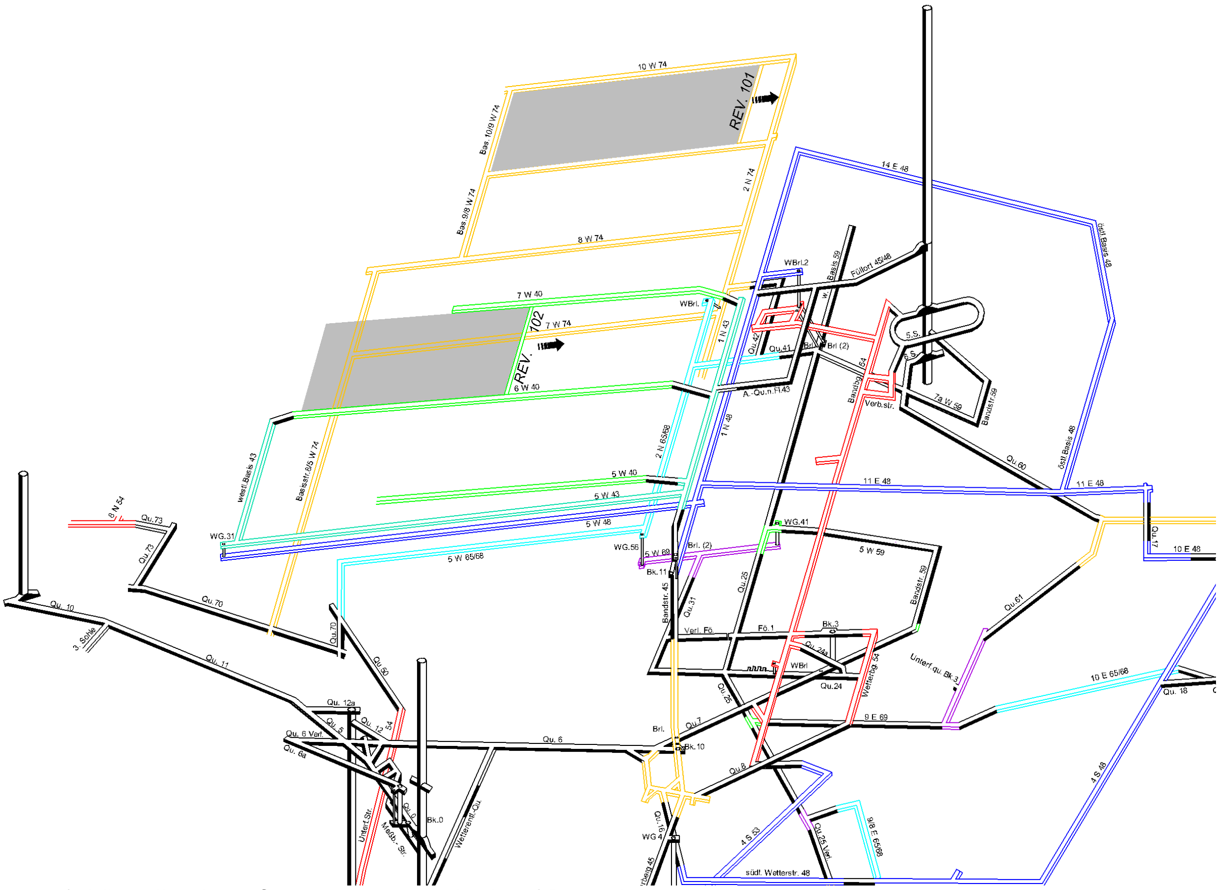


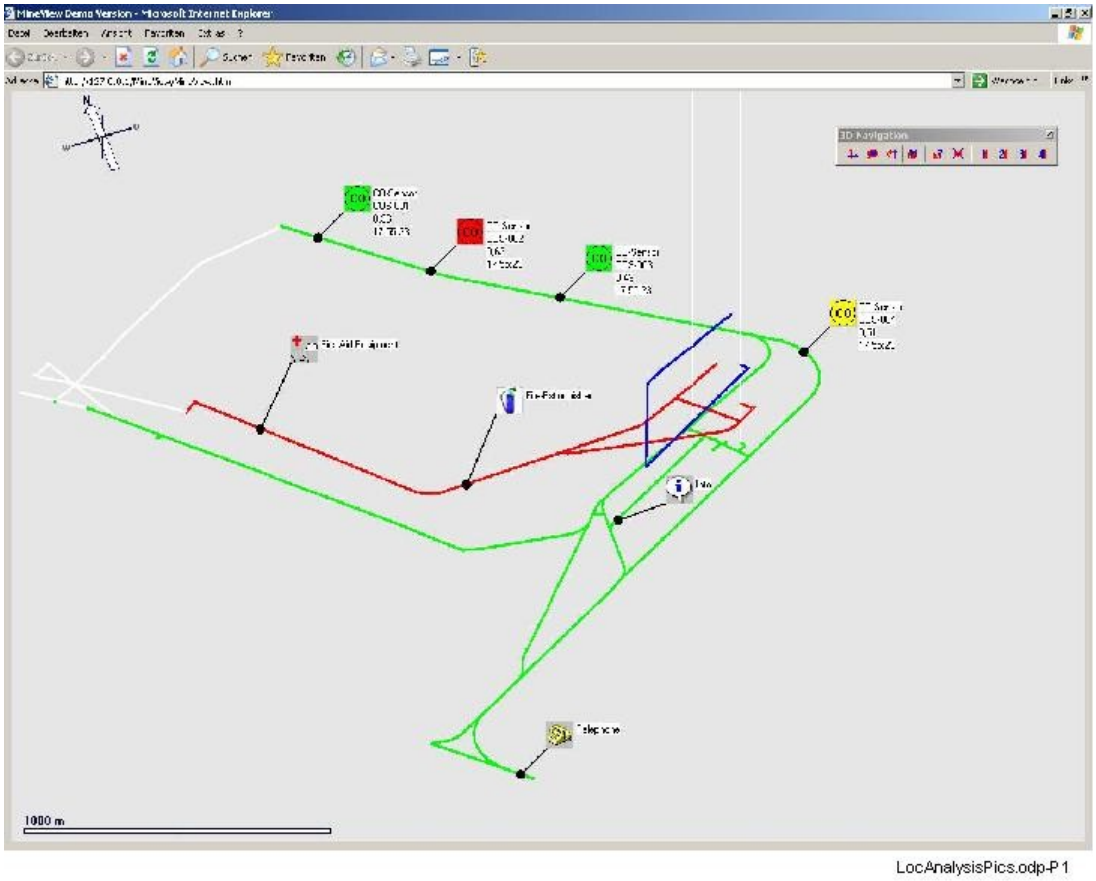
Figure 1: Visualization of an underground mine 3D model

can see the on-line electricity status or other operational data in a location based context as displayed on the screen shot in picture 1.

Such software tools also are used for ventilation simulation and calculation as well as for visualization of the gas concentrations in the mine[54].

The mine model as such is basing on nodes and vectors, where a node typically is a position and a vector is representing the interconnection between two positions. Each position is assigned a 3 dimensional coordinate (x,y,z) and thus also the vectors have three dimensional properties[54].

At any point in the model which falls on a vector or on a node position, certain additional information can be hooked up. This is typically performed using multiple layers in order to structure the information. If these layers contain dynamic process information, a dynamic online visualization is created. This is by example the case in the MineVIEW 3D software from XGraphics GmbH [54]



Picture 1: Location based mine visualization in MineView

1.2 Underground Mine safety

1.2.1 Introduction

Underground mining means to work in a potentially dangerous environment. Mining accidents often cause loss of life of numerous people. In the USA alone 35,4 people were killed in coal mining accidents in the annual average from 2006 until 2010 [162]. In non coal mining, the number of fatalities is significantly lower (24,2 in the average from 2006-2010 [162]). This difference is mainly caused by the additional risks of coal mining mainly as these mines are exposed to the additional danger of methane gas explosions. This underlines the extraordinary importance of improved safety especially for underground coal mining.

Due to the immanent danger of methane explosions in coal mining however, all electrical and electronic equipment used has to be protected or designed to meet the rules of explosion protection or intrinsic safety.

In each mine, rules apply for emergency handling and evacuation. These rules are set up basing on national law and rules imposed by the safety authorities. In this context it is important

to realize that these rules are not identical in every application. They also can be contradictory between different countries and even between different states as in the USA.

As this document cannot mirror the complete global legislation it gives an introduction on the situation inside the EU and in Germany in particular as well as in the USA where new legislation activities were started after mining hazards in 2006 and 2007 and which therefore can be regarded the most up-to-date approach on mining safety legislation.

1.2.2 Regulations on European Union level

In the European Union there is neither a harmonized legal basis for underground safety in general nor for underground communication systems in particular. Consequently, the regulations concerning underground safety therefore are covered by individual legislation and rule-making in each single member state.

The only exception to this is the approval procedure for Explosion proof equipment for use in coal mines in accordance to the Directive 94/9 EU, also called "*ATEX Directive*".

Certain member states have their individual rules for mine communication systems. Therefore a general evaluation on resilience factors can only be carried out basing on rules and requirements available for other industries (see chapter 3.1).

The applicable legal basis on European level (superceding national regulations) which is of general importance for any workplaces (not limited to mining) conforms of:

1. EU Directive on occupational safety and health 89/391/ EC [38] in the newest revision as of 2009 [42]
2. EU Machine directive 2006/42/ EC[39]
3. EU Low Voltage directive 2006/95 EC[43]
4. EMC-Directive 2004/108 EC[40]
5. EU-Explosion protection ("*ATEX*") directive 1994/9/EC[41]
6. IEC/EN 61508 functional safety norm and derived norms[62][63][64][65][66][67][68][69]

Article 8 of the „*EU Directive on occupational safety and health 89/391/ EC*" clearly states that [38][42]:

"*1. The employer shall:*

- take the necessary measures for first aid, fire-fighting and evacuation of workers, adapted to the nature of the activities and the size of the undertaking and/or establishment and taking into account other persons present[38],

...

3. The employer shall:

(a) as soon as possible, inform all workers who are, or may be, exposed to serious and imminent danger of the risk involved and of the steps taken or to be taken as regards protection[38];

(b) take action and give instructions to enable workers in the event of serious, imminent and unavoidable danger to stop work and/or immediately to leave the work place and proceed to a place of safety"[38].

In the mining context, this sets high demands on the availability of communication especially in cases of emergency. This leads to the interpretation, that "*due to the size and nature of operations*" a mining communication system regardless of it's kind is to be regarded a safety component of the operations.

This fact in combination with the norms basing on IEC EN 61508[62] covering functional safety may lead to an applicability of these group of norms to any kind of safety related underground communication.

This is already the case if machines are operated under ground forwarding control commands via electronic communication systems. The new EU machine directive as enforced from 2010-01-01 includes all steering related communication into it's scope[39][45] (§ 1.2).

The newest list of harmonized norms to the machine directive as of 2009-12-18[44] states a number of technical standards assuming the coverage of the machine directive if the norms are met. In this list, no mining specific norms are covered with some connection to underground communications.

In general legislation practice, directives set by a higher body usually superceed lower level regulations. Therefore, EU legislation superceeds national legislation of the EU countries which in turn superceeds state legislation which has a higher ranking than local or company rules. This needs to be known while evaluating the national legislation.

1.2.3 Regulations in Germany

In Germany, the legislation is basing on the federal mining act ("*Bundesberggesetz*") [48]. Basing on this act and a secondary general mining rule ("*Allgemeine Bundesbergverordnung*") [47], each state imposes regional rules to apply for the mines within the particular region [128] [79]. These rules also implement related directives imposed by the European commission.

The "*Bundesbergverordnung*"[47] furthermore manifests in §2-4 general rules for performing underground works. In Number 4 this section states that "*with all measures the current technical state of the art...*" has to be taken into account which gives a big potential for official implementation of the results from this thesis as soon as they can be proven to be the new state of the art.

Details about how to handle mining operations in particular can be found in the "*Bundesbergverordnung*" [47]. Articles relevant for communication, evacuation and safety include the following main topics:

- Any underground operation has to have two independently accessible exits leading to surface "*easy to access for the personnel*" (§15-1).
- From any workplace in the mine two exists have to be accessible. A dispense is only made for areas in development where by nature only one exit is possible (§15-2).
- All underground workplaces have to be equipped in a way that the danger for workers while working and while riding to the workplaces is minimized (§15-3).
- Drifts and tunnels are equipped with markings to assure orientation for people (§15-3)
- Communication to the workplaces by telephone or radio reduces the necessity for the supervisors to visit each workplace (§5-3).
- The required communication aids for Search and Rescue operations are available and functional (§11-1)

the attachment 4 to this document "*Anforderungen an die Sicherheits- oder Gesundheitsschutzkennzeichnung*"[46] ("*demands on signalling for safety and health*" contains minimum requirements on signalling and marking of safety and healty relevant works. This document states in article 1.1.2.1 that "*a communication concerning dangers and distress calls to persons .... e.g. for evacuation ... can be performed by visual or audible signals or by verbal communication*".

Concerning survivability in case of power loss it is only stated in article 1.5.3 that

"*Signals which need a power source have to be equipped with an emergency power supply in case the regular power fails...*"[46]

Following these federal regulations imposing general minimum requirements, each state has created an own legislation dedicated to the needs of the mines in the state area. For this evaluation, the rules of the major mining state Nordrhine-Westphalia shall be taken into account. These rules are covered mainly by the "*Landesbergverordnung*" ("*State mining directive*") and subordinated documents which contain the following regulations with relation to communications:

	Regulation, Requirement	Source
1	**Signaling instrumentation for hoisting and transport equipment** *"Förder- und Transporteinrichtungen sowie Einrichtungen zur maschinellen Fahrung müssen mit einer Signalanlage ausgestattet sein, wenn sie nicht vom Bedienungsstand aus zu überblicken sind. Erforderliche Signalgeber und -empfänger sind in angemessenen Abständen anzubringen."*	State NRW: BvSt (2001), §43 (3) [77]
2	**Telephones close to workplaces in drifting operations** *"In den in Auffahrung befindlichen Grubenbauen muss eine Fernsprechanlage nahe am Arbeitsplatz vor Ort vorhanden sein."*	Federal: BVOESSE (2001) §46 (1) [129]
3	**Early warning of people in case of an incident** *"Eine frühzeitige Warnung der Beschäftigten im Falle eines Ereignisses muß sichergestellt sein."*	State NRW: Escape route directive ("*Fluchtwegerichtlinie*"[76], Article 3.2
4	**Early warning of people in areas covered by auxiliary ventilation, requiring two way voice communication close to workplaces and along the trafficways in the auxiliary ventilated area** *"Durch geeignete Maßnahmen muß sichergestellt sein, daß bei einem Ereignis alle Personen in sonderbewetterten Betrieben und Raubbetrieben sofort gewarnt werden können. Eine Zweiweg-Sprechkommunikationseinrichtung mit optischer und akustischer Signalgebung muß im Vorortbereich vorhanden sein.* *Weitere Kommunikationseinrichtungen müssen am Eingang sowie in geeigneten Abständen entlang des sonderbewetterten Bereichs eingerichtet sein. Um sicherzustellen, daß die Warnung die betroffenen Personen jederzeit erreicht, muß die Möglichkeit bestehen, sich von einer ständig besetzten Stelle (z.B. Sicherheitswarte) aus auch in laufenden Gespräche einzuschalten.*"	State NRW: Escape route directive ("Fluchtwegerichtlinie"[76], Article 3.12
5	**Two way voice communication along conveyor belts** "*Durch Zweiweg-Sprechkommunikationseinrichtungen (z.B. Lautsprecher-Wechselsprechanlagen) in ausreichender Anzahl ist sicherzustellen, daß alle durch einen Brand gefährdeten Personen in den Grubenbauen mit Gurtförderern sofort gewarnt und zurückgezogen werden können.*"	State NRW: Appendix 1 and Appendix 3 to the Escape route directive ("Anhang 3 zur Fluchtwegerichtlinie")[76]
6	**Early warning in case of emergencies** "*In einer Notsituation muß die davon betroffene Belegschaft eines Bergwerks unverzögert gewarnt werden können. Die Untertagebelegschaft muß Möglichkeiten zum unverzüglichen Verlassen des Grubengebäudes nach über Tage haben. Der Unternehmer hat die hierzu notwendigen Maßnahmen zu treffen und die erforderlichen Anlagen einzurichten (§ 61 Abs. 1 BBergG).*"	State NRW: Directive "Sicherstellung der elektrischen Energie-versorgung und Warnung der Belegschaft"[75]Article 2

	Regulation, Requirement	Source
7	**Cabling for telephones shall be drawn via two shafts with failover function, as long as this is not possible, phones and safety related measuring devices equipped with battery backup.** "*Es ist anzustreben, auch die Kabel und Leitungen von Fernmeldeanlagen und das Fernmeldenetz entsprechend Abschnitt 3.2 Absätze 1 und 2 auszulegen und zu betreiben.* *Soweit im Einzelfall die Anforderungen nach den Abschnitten 3.1 und 3.2 noch nicht erfüllt sind, müssen mindestens Fernsprechanlagen und Anlagen zur Übertragung sicherheitstechnischer Meßwerte (Fernmeldeanlagen) eines Bergwerks bei Ausfall der übertägigen Energieversorgung betriebsbereit bleiben, zum Beispiel durch Versorgung durch Akkumulatoren oder mittels Generatoren. Fernmeldeanlagen in Grubenbauen, in denen in Notsituationen nach Abschnitt 1.1 oder bei Stillstand der Sonderbewetterung mit Grubengasan-sammlungen zu rechnen ist, müssen - soweit technisch möglich - so beschaffen sein, daß sie nach den bergbehördlichen Vor-schriften in diesen Grubenbauen weiterbetrieben werden dürfen.*"	State NRW: Directive "Sicherstellung der elektrischen Energie-versorgung und Warnung der Belegschaft"[75], Article 4.1
8	**Interruption of a phone cable via one shaft as well as partial failure of one phone center may not result in disconnection of all underground phones. In important places two phones shall be available, each of which connected via another shaft.** *"Fernsprechanlagen sind über mindestens zwei Schächte, davon mindestens über einen Einziehschacht, zu führen. Bei Unterbrechung einer Fernsprechverbindung in einem Schacht muß die Fernsprechverbindung von über Tage nach unter Tage gewährleistet bleiben. Ein Teilausfall der Vermittlungseinrichtung darf nicht zum Ausfall aller untertägigen Fernsprechgeräte führen.* *An wichtigen Stellen des Grubengebäudes (z.B. an Anschlägen der Seilfahrtschächte, an Zugängen zu den Förderbergen, in Schachtanlagen, an Zentralladestellen, in Werkstätten) sollen zwei Fernsprechgeräte vorhanden sein, die jeweils über getrennte Leitungswege anzuschließen sind. Statt dessen genügt ein Fernsprechgerät, das über eine Zusatzeinrichtung an zwei Zuleitungen angeschlossen ist; im Fehlerfall muß die ungestörte Zuleitung automatisch wirksam werden."*	State NRW: Directive "Sicherstellung der elektrischen Energie-versorgung und Warnung der Belegschaft" [75] Article 4.2
9	**Warning of workers under ground by optical and acoustic means and voice communication** *"Es ist sicherzustellen, daß in Ausrichtungs-, Vorrichtungs-, Gewinnungs- und Raubbetrieben sowie im Förderbetrieb in einer Notsituation gefährdete Personen unverzögert und jederzeit durch geeignete optische oder akustische Einrichtungen gewarnt werden können. Diesen Personen müssen die notwendigen Weisungen über eine Fernsprechanlage, z.B. Selbstwähl-, Wechselsprech- oder Lokfunkanlage, gegeben werden können; für diesen Zweck sollte die Möglichkeit bestehen, sich von einer ständig besetzten Stelle aus (z.B. Sicherheitswarte) auch in laufende Gespräche einzuschalten.* *Die gleichzeitige Alarmierung gefährdeter Personen sollte durch Gruppenrufsysteme oder andere Systeme verbessert werden. Es ist anzustreben, auch an abgelegenen Arbeitsplätzen, z.B. auf alten Sohlen, Fernsprechanlagen zu betreiben."*	State NRW: Directive "Sicherstellung der elektrischen Energie-versorgung und Warnung der Belegschaft"[75] Article 4.3

Table 1: Communication regulations for coal mines in NRW

These regulations describe in a quite detailed form the functional needs for underground communication however they do not imply a certain communication system hardware to be used.

1.2.4 USA

For comparison, a short introduction shall be given to the legislative situation in the USA as this is referenced later in this report.

Especially following the hazardous coal mine accidents in the USA in 2006 and 2007, federal and state legislation has been set in force to assure post accident communication and tracking of miners under ground[164]. Additionally, state legislation applies. However, at the time the new legislation was put in force, only vague ideas were available on how the new legal requirements could be met in practice, leading to accelerated research and testing activities of the related institutes NIOSH and MSHA, especially covering underground communication (see chapter 3.2).

Now in fact the USA can be regarded the country with the currently widest reaching legal demands on underground communication. However, especially in coal mining, the use of technology is partly blocked and delayed by the fact, that the national certification of intrinsically safe equipment does not follow any international norms limiting the availability of equipment to few suppliers. In this case two legislative demands in the USA seem to partially block each other and prevent modern and proven safe equipment to be used in the USA.

In an act proposed by the US Congress in 2007[163], R&D activities related to underground communication were proposed. Among the items proposed are:

- "Systems that are likely to work in emergency situations
- systems that provide coverage throughout all areas of the mine
- hybrid systems that use both wireless and infrastructure-based systems
- systems that serve emergency and routine communications needs"

This proposed act never became US federal law, however it shows clearly the identified need for related systems.

1.2.5 Experience from mining accidents

Underground mining accidents can be classified in an escalation hierarchy as follows:

Working Accidents: One or few people involved, mining infrastructure intact, communication needed to call for help and to organize help to potentially injured people.

Important due to distances under ground. First aid can be organized locally, no danger of emergency escalation

Emergency: Accident caused by external influence not directly related to the work of people: Fire, gas explosion or roof collapse in a certain area of the mine. The main infrastructure remains intact, Communication between above ground centers and people in field is still possible. The situation most probably can be controlled by the regular safety procedures with assistance through mine safety forces. An escalation of the situation to other areas is not probable. Few people may be trapped.

Hazard: Major destruction to the mine infrastructure (tunnels, shafts etc), Miners potentially trapped, larger number of fatalities to be expected. An escalation to the entire mine or major parts of the mine cannot be excluded.

The main causes of Emergencies and Hazards are[172]:

1. Rockfall or rockbursts
2. Fire
3. Gas explosions
4. Water intrusions
5. Loss of ventilation

In general, modern communications are not able to prevent from the physical cause of an accident, however it can help to:

1. Evacuate miners from the mine by letting them know about the danger using voice communications or loudspeaker systems[76]
2. Actively guide miners to exits
3. Store the locations of the miners on servers above ground, so it is known where the people were before the accident occurred. Such systems are partly implemented today.
4. Let the miners underground know where everybody is in order to organize self-escape without leaving people behind (part of the EU EMTECH project this thesis basis on[16])
5. Conduct target oriented Search-and-Rescue operations basing on the latest or current locations of the miners[16].

Analyzing latest mining accidents in this context concludes that reliable communications are needed to successfully handle mine emergencies successfully[144] in order to prevent from or to minimize the number of fatalities. Also communications is of highest importance for the rescue teams in case of an Emergency or Hazard situation[126].

This highlights the need for a resilient communication system which has a high chance to at least partly survive accidents and to stay functional in those extreme situations[144][164][163][34].

The notification presumes that a communication still is possible which may not be the case due to the traditionally high salvage-ability of communication systems[33].

Despite the fact that in many cases the availability of a communication system may have helped people under ground to evacuate safely[144] also the newest legislation in terms of general safety and health at work has to be taken into consideration when designing future systems (see chapters 1.2.2, 1.2.3 and 1.2.4).

In case of an emergency, also the existing rules and guidelines experience their limits in practical applicability, which is explained in brief by some examples:

The rule to mark the tunnels with emergency exit signs for better orientation[76] is not clearly visible under ground: In practice mostly the signs are covered by layers of dust so their existence can hardly be imagined. Especially under stress conditions it would be very hard to find a suitable exit just by following underground signs.

Additional rules say[76] that people always should escape against the air flow in order to reach an air intake shaft and to stay in oxygen rich air. But what, if the accident has blocked the fresh air stream? How to reach a fresh air stream then? Where is the closest fresh air stream? This could have changed dramatically following tunnels collapsed after an underground disaster.

The need for two independent underground escape routes is the basis for the dynamic evacuation guidance discussed later in this thesis.

1.2.5.1 Handling of accidents with relation to communications

The handling of safety cases in mining can be classified in the following escalating phases:

1. Prevention of accidents so the probability of an accident is reduced. This is the aim of

all safety related mine operational rules and directives[47][48][164][141].

2. Fast local response: When an accident or irregularity has happened, the people present on site have to be enabled to handle the situation so it does not extend or worsen. This is performed e.g. by distributed fire fighting equipment or first aid equipment available. At the same time, they have to communicate the situation to all relevant people[19].
3. If a fast response is not possible or ineffective, saving life is the major task. People move to an emergency exit or to a safe shelter ("*Self escape phase*")[19], where they wait for rescue teams to arrive.
4. If people under ground are not able to deal with the situation by self escape, they need "*assisted rescue*" which means that special rescue teams are called in for rescue of life as primary task and for dealing with the situation (e.g. fire fighting) as secondary task. This has been visible worldwide by the rescue of trapped miners in the Chile mine accident in 2010 [173].

In the USA there is no fixed rule for double exit layouts which was one of the reasons for many fatalities in recent mine accidents ("*Sago Mine*" 2006 [126]etc) where miners surviving the disaster got trapped and were not able to escape.

In today's state of the art, safety related underground electronic systems are not interconnected with each other. All information is collected from every systems independently on servers above ground. Therefore, a complete situation overview only exists above ground and only if the cables are not affected by an underground accident: Normally, each safety system (Ventilation data, gas sensors) has a separate and dedicated set of communication cables. These are dedicated, non redundant cables in a tree structure.

Consequently, if the sensor cables to above ground are cut, neither the operators nor the safety people above ground know about the situation, nor the workers underground even if the telephone line is still working. If telephone lines are cut but the sensor cables are not, people above ground know about the situation but the workers under ground (who most urgently would need e.g. the gas sensor information) cannot be informed about how to behave. Underground, there is no local access to this information which in case of an emergency could be used e.g. to tell the people where to find the next fresh air stream or the next exit which is the topic of the following chapters.

1.3 Functional Safety

Most of the current legislation concerning mine safety and communications was created and applied before standards and legislation relating to functional safety of technical installations became originally applicable e.g. with the norms of the IEC/EN61508[62] group of international standards in the late 1990's.

Today, also other norms relate to requirements in functional safety as e.g. the EU machine directive[39][45] or the norms to apply the EU ATEX directive[41]. Also other legislation like the EU directive of safety and health at workplaces[38] set high demands on the information of workers in case of accidents.

In terms of underground mining communication systems, research was carried out within the EMTECH R&D project to assess the degree of functional safety required for underground communication systems[19][20]. The results can be summarized as follows:

IEC 61508, the other related standards and the Safety Integrity Level (SIL) assessment techniques employed by them are designed to assess and/or minimize risks to health and safety. Essentially, this is achieved by establishing the Safety integrity of systems. Safety integrity is defined in IEC 61508 as:

"*The probability of a safety-related system satisfactorily performing the required safety functions under all stated conditions within a stated period of time. The higher the level of safety integrity, the lower the probability that the safety-related system will fail to carry out the required safety functions."*[62]

SILs are defined as:

"*A discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the safety-related systems, where level 4 has the highest level of safety integrity and level 1 has the lowest.*"[62]

Example SIL assignment methodologies can be found within IEC 61508 and the industry specific standards and guidance documents that have evolved from them. In essence all of the example approaches involve calculating the frequency of a hazard and the magnitude of its consequences to determine the difference between the existing risk and the "*tolerable risk*"[19].

Given that communication systems should never be able to directly initiate events that are hazardous to health and safety, safety cases which cause loss of life due the unavailability of

communication have to be evaluated as the worst case conditions for the functional safety assessment.

Basing on a general example by Smith/Simpson[151], an attempt was made to quantitatively assign the potential SIL level for an underground communication system basing on easy to reproduce and easy to understand information.

The calculation bases on the German mining statistics for 2009[21], using the following base information from this source:

- Number of coal mines in Germany: 6
- Number of registered accidents total: 260
- Resulting number of registered accidents per mine (average): 260 / 6 = 43,3

Furthermore, the following assumptions, simplifications and preconditions are made for the calculation:

- Every registered accident conforms an acute, real danger for life or health
- If the communication system fails, it fails completely and no call for help is possible from another station nearby
- Delayed communication (a person walks or drives until it finds a working communication unit) is impossible and leads to fatality
- Alternative communication systems are not available or not functional
- The communication system is the only possibility to help the person, meaning e.g. that rescue equipment on site is not available

Under these assumptions the availability of the communication system is the only decisive factor for health recovery in case of an accident. Consequently, the resulting SIL level depends on the number of hours the communication system is unavailable and the probability that an accident occurs during this time:

Availability of the communication system	Hours per year the comm system is unavailable (rounded)	Accidents left handled improperly per year PFD
90,00%	8760 x 0,1 = **876**	876 / 202 = **4,33**
99,00%	8760 x 0,01 = **88**	88 / 202 = **0,435**
99,90%	8760 x 0,001= **9**	9 / 202 = **0,044**
99,99%	8760 x 0,0001 = **1**	1 / 202 = **0,005**

Tabelle 2: Maximum probability of a dangerous failure for an underground communication system

From these calculations the resulting SIL level can be derived under the preconditions stated above:

Accidents left handled improperly per year PFD	Probability of failure on demand PFD allowed (EN61508)	Resulting SIL level
876 / 202 = **4,33**	$\geq 10^{-1}$	SIL 0
88 / 202 = **0,435**	$\geq 10^{-1}$	SIL 0
9 / 202 = **0,044**	$\geq 10^{-2}$ to $< 10^{-1}$	SIL 1
1 / 202 = **0,005**	$\geq 10^{-3}$ to $< 10^{-2}$	SIL 2

Tabelle 3: SIL class resulting from failure probability

This means that a target SIL class for a mine communication system under the preconditions stated above should be SIL1. This also meets quite well the example by Smith/Simpson[151], even if the assumptions for the concrete calculation have been additionally simplified.

It sets the demand on the communication system for an overall availability of 99,9%.

1.4 Mine Communications

1.4.1 Purpose of mine communications

Communication in underground mines fulfills a number of purposes for organization of the production processes, in mine logistics and for the mine workers safety.

In particular, the following applications have to be covered by a mine communication system:

1. Automation and remote control of stationary devices, mainly via field bus systems[143]
2. Remote Control of mobile equipment[170]
3. Supervision of autonomous mobile equipment[170]
4. Environmental and gas sensors and data acquisition (only for use by central systems today, for use in the field selected people wear their own personal gas sensor devices) [78]
5. IT (Access to Intranet) for underground offices and mobile staff[56]
6. Video surveillance for CCTV systems[56][170]
7. Telephony[76][19]
8. Interkom (Loudspeaker systems)[73][19]

1.4.2 Traditional Mine Communication Systems

Traditionally, various hard wired and wireless mine communication systems are available on the market. These systems differ in the use of their physical communication infrastructure as well as in the communication protocols used[19][130]:

Voice communication:	Telephony
	Low frequency audio communication (2-wire based Public address)
	Wireless VHF or UHF band radios („walkie-talkies“)
Data Communication:	Telephone Modems
	RS485 based systems (proprietary and e.g. PROFIBUS)
	Point-to-point fiber links with special converters
Video Surveillance:	Analog cable-TV systems
	Dedicated fiber optic links

1.4.2.1 Telephones

Traditional telephone systems are installed in nearly any underground mine and their installation is also mandatory in most cases[76][129]. They are characterized by a hierarchic cabling structure. When a main trunk cable is cut (e.g. following a mine emergency), the entire communication of all phones connected to this trunk lines is interrupted.

As the system is unable to be set up in a redundant way, certain regulations demand two telephones in one location, where each of those is to be connected to above ground via different shafts[75].

1.4.2.2 Leaky Feeder Systems

Special mining communication systems are mostly basing on derivatives of coaxial cable as a carrier medium using analog cable TV technology as a transportation technology[19]. Such systems are in the industry known as "*Leaky Feeder*" systems[171]. The power supply for active field components is distributed as an DC voltage coupled onto the coaxial cable. The resulting advantage is that only one single cable has to be used for the entire system. Wireless components are connected by using radiating coaxial cable as a carrier medium rather than fully shielded cable.

The advantage of such systems is that standard handheld communication radio devices using the VHF or UHF bands directly can be used with these mining communication systems.

The disadvantages of such systems are the requirement of equipping all the mine with expensive radiating cable (depending on quality abt. USD 10.000 per km) plus the proprietary and expensive technology used which is not compatible with modern networking technologies. Furthermore, these systems mainly can be used for voice and analog video. Their use for data communication is limited in practice so additional dedicated links using field buses etc. are additionally required[130].

1.4.2.3 Loudspeaker Systems

Especially along conveyor belt systems and in other wide spread working locations like in coal mining longwalls, loudspeaker systems are mandatory. These systems work as intercom systems where a dispatcher above ground is able to send messages to all connected loudspeaker stations. On each of those stations a worker also is able to talk to all other loudspeakers and to

the dispatcher by pushing a microphone button[73]. The communication is half-duplex.

In most cases, the signals in these systems are transferred using telephone cables. The logic setup does not contain redundancy measures to allow a redundant cable connection to above ground[130].

1.4.2.4 Safety related Data Communication Systems

Safety related data communication covers all data communication with some relation to mine safety. This is especially the remote monitoring of gas sensors (CH4, CO and others) as well as ventilation data (air speed, air temperature etc)[130].

These systems are traditionally installed since many years using a low speed data communication basing on serial interfaces or tone frequency modulation using telephone cabling. In nearly all of these systems regular phone cables are used to link the devices with data concentrators or processing devices[130].

One EU directive already today covers functional safety: The "*EU Machine directive*" 2006/42/ EC[39] handling functional safety of machines refers to the norm IEC EN 61508[62] for performance of risk analysis and for the design of safety related equipment. This directive is mandatory for all mining equipment but not for mining operations in general.

However it can be regarded a good engineering practice to apply relevant parts of this directive for use as a non normative guideline to design up-to-date safety related underground communication systems[130].

In connection with the demands of the directive 2009/104 EC[42] and 89/391 EC[38] it is clear that all technical progress has to be used to assure occupational safety and health which also is mirrored by a number of national regulations[130].

1.4.3 Resilience of traditional mine communication systems

Within a study prepared for the EU EMTECH project[130], the resilience of the traditional communication systems was assessed. For this purpose, questionnaire was prepared which was filled in by major European mining companies[130].

The results of this research were evaluated against the following technical factors of resilience:

1. Resilience of the power supply
2. Resilience of the cabling
3. Resilience of the data processing and availability of central (above ground) functions

1.4.3.1 Power Supply resilience

As a result from the questionnaire it can be concluded that all safety relevant units are equipped with battery backup power supplies. The independence time of such battery backup varies substantially between 1 hour and 12 hours.

From this point of view the systems can be regarded robust enough and up-to-date in terms of functional robustness[130].

1.4.3.2 Cabling resilience

The reliability of the communication functionality is also dependent on the reliability of the cabling between the active components or between an active component and the central processing unit. The latter one in case of phone communication is a central phone switchboard („PBX“)[130].

The analysis of the questionnaire in terms of the cabling structures used shows that in most cases cabling structures are set up in star structures where dedicated cables are used between the central processing unit (switchboard) and every single terminal (phone)[130].

This is a highly salvageable setup as an interruption of a trunk line containing a large number of cables would leave an entire mine - if the interruption occurs close to a shaft or at least entire mine areas without communication[130].

It was common practice in traditional communication systems to use joint cable trunk lines of phone cables for both phones and tone frequency coupled or serial data communication for environmental and gas sensors. Therefore in case of a trunk line damage, both voice and data communication most probably are lost[130]!

This is in principle not enhanced by introducing underground data concentration units for sensor information. The use of such data concentration as cable multiplexer just minimized the numbers of wires needed in the trunk lines[130].

In principle, these results also apply to the Interkom systems reported: In these systems,

the loudspeaker units are connected in a single ended chain of devices. In 8 out of 12 systems reported all interkom (loudspeaker) units behind a cable interruption are dead. Three systems did not report on this issue and for one system the reporting was inconsistent stating both „*dead*“ and „*supplied from the other end*“. This result also relates to Leaky Feeder systems[130].

Five out of 12 systems are reported to at least be able to detect and report cable interruptions[130].

Systems using redundant central units with dedicated cables from each terminal to both switchboards for redundancy reasons are not used in practice[130].

Therefore, the missing cabling robustness can be regarded the Achilles' heel in any kind of safety related underground communication today.

1.4.3.3 Data Processing Resilience

All the information acquired by any underground sensors is important for the health of the workers under ground. However this raw sensor data traditionally is only forwarded to central systems above ground, where the data is interpreted and turned into usable information. Due to the processing above ground the information is not directly accessible by the workers under ground. If this is needed, the information is then communicated back to underground. Consequently, much of the sensor information cannot be seen directly by the miners working in this area[130], if not e.g. the measuring device is equipped with a small local display.

To inform the miners about a dangerous situation, all communication from the sensor to above ground, the processing system above ground and the Interkom- or phone communication under ground have to be functional[130]!

This leads back to the crucial cable robustness because the data cabling often is embedded inside the phone trunk cables so a damage of a trunk phone cable would probably result in loss of environmental data access and at the same time in the loss of the ability to inform the people under ground[130].

1.4.3.4 Resilience of traditional communication systems

The results of the EMTECH study can be summarized in the following table:

Criterion	Phone	LeakyF	Interkom	S-Data
Required by law	YES	NO	PARTLY	YES
Power supply robustness	GOOD	GOOD	GOOD	GOOD
Cabling robustness	**POOR**	**POOR**	**POOR**	**POOR**
Processing robustness / local accessibility	**POOR**	**POOR**	**POOR**	**POOR**

Table 4: Resilience of traditional underground communication systems

From the power supply redundancy point of view the traditional systems can be regarded as „*up-to-date*“ in terms of safety demands.

These survey results show that none of the communication systems used for safety related underground communication today complies with up-to-date technical possibilities nor with safety related regulations applicable in other industries. This especially relates to the resilience of all the cabling systems used. Furthermore, there is no or only limited local accessibility to the safety sensor information communicated via these systems.

The missing robustness in cabling and the insufficient processing and system robustness are system immanent, a further development basing on the traditional technologies would be too expensive and unnecessary due to standard alternatives available.

It is thereby obvious that the traditional systems cannot fulfill today's demands on safety and health and functional safety as demanded by current legislation (see chapters 1.2f) and with today's technological possibilities (see chapter 2ff).

1.4.4 International Studies on Mine Communication Survivability

Recent studies being undertaken in the US by CDC NIOSH (“*National Institute for Occupational Safety and Health*”) and MSHA (“*Mine Safety and Health Administration*”) have been assessed comparatively along with earlier studies in Australia, Canada, Japan, South Africa and elsewhere. One key observation from these studies is the impact that the method of mining has on the requirements for mine communication system coverage and therefore the response to various failure modes arising after a major incident.

In 2007, Synder[156] and Harris[51] have assessed communication infrastructure and future options appropriate to the continuous miner sections and multi-entry longwall mining practices in the US. It is evident that system failure modes and their impacts in the US can differ

from the requirements and impacts in the EU. The US studies have concentrated on:

1. Assessing quality of communication
2. System functionality and coverage
3. System survivability and failure modes
4. Identification of alternative or hybrid technologies to enhance survivability and meet the minewide coverage requirements of the US MINER Act[164].

Communication Technology	Greatest Potential	Current Position
Through The Earth (TTE) 200Hz - 4000 Hz	No in-mine backbone	Commercial one-way with text Off-axis reception problematic Large antenna loops Non-permissible power requirements Emergency refuge option
Medium Frequency (MF) 300 kHz - 3 MHz	Use of existing mine cable infrastructure as backbone Interoperability	Early MF systems now obsolete New technology prototypes demonstrated Unknown safety
Wi-Fi Mesh Nodes 2.4 GHz	Wide bandwidth and flexibility Interoperability	Prototype - early commercial systems demonstrated Limited node-to-node range Line-of-sight only Handsets not commercial Requires redundancy and hardening
Leaky Feeder (VHF) 150-170 MHz Distributed Antenna System	Available and upgradeable Interoperability	Multiple installations Commercial handsets Limited beyond sight of feeder Limited data capability Requires redundancy and hardening
Leaky Feeder (UHF) 400-500 MHz Distributed Antenna System	Available and upgradeable Interoperability	Multiple installations Commercial handsets Some use beyond sight of feeder Moderate data capability Requires redundancy and hardening
Leaky Feeder Enhancements Multiple Distributed Antenna Systems	Mine wide coverage Multiple pathways	Limited installation experience Prototype only, technology development requirements

Table 5: Comparison of wireless communication technologies for coal mining[51]

Functionality and survivability reviews conducted on behalf of MSHA (at Federal level) and the West Virginia Office of Miners' Health, Safety and Training have involved the assessment of various communication techniques for their technical limitations, potential for further development/application, and survivability profile. This work is summarized in table 5.

Unfortunately, this report only focuses on completely wireless systems. Hybrid systems (e.g. consisting of a hard wired backbone and wireless access) are not covered by this report.

Overall conclusions suggest the following for the USA:

- Interoperability between systems is limited
- Solutions are often site specific
- Further development of technologies is required.

The approaches considered to offer the greatest potential in terms of system survivability involve:

1. Engineering multiple pathways
2. Engineering system integration
3. Engineering systems which will adapt and use whatever transmission path survives.

1.5 Early approaches to unified mine communication systems

1.5.1 Motivation

In mining, infrastructure cost is essential. Thus, a communication system should be a multi purpose system capable of transferring all types of information as data, voice and video on one single infrastructure.

Many attempts have been made in the past two decades to achieve the goal of integrative communication, which are briefly outlined in this chapter. Retrospectively it is important to realize that these systems were developed long before the Internet technologies with their "self evident" integration of all communications became available.

All these systems have in common their motivation for an unified communication system which provides significant benefits in investment cost compared to the design and installation of multiple separate, dedicated systems.

During operation the benefits are in the fact that only a single system has to be maintained which results in a significant reduction of the life cycle cost.

1.5.2 Siemens OTN

OTN stands for Open Transport Network. It is a fiber-optic networking technology which integrates data, voice and video telecommunications needs[147]. It is a proprietary system from Siemens providing interfaces to all kind of standard communications.

It bases on a redundant fiber optic ring topology with very long distances (up to 140km) possible between two network nodes[147].

OTN is used in the mining industry mainly in open cast mining operations[148].

1.5.3 COM2000 (LKAB)

Due to the lack of availability of a unified communication system with wired and wireless components at that time, the Swedish iron ore manufacturer LKAB developed their "*COM2000*" system during the 1990's basing on ATM technology and fiber optic backbones. The wireless part was implemented using a link aggregation of several GSM channels. The system was provided by the Finnish company Elektrobit which also developed the system together with and specifically for LKAB[170].

Using this system, machines like Drill Rigs and loaders were remotely controlled and operated autonomously[170].

All such individual projects have in common their individual design resulting in high cost for development, implementation and service. In addition their overall lifetime is limited as the obsolescence of electronic components soon causes redesigns which cannot be financed individually. Due to this fact, LKAB today is using mainly Ethernet based infrastructure.

1.6 Ethernet in safety related architectures

At the same time, new technology has evolved in the area of commercial networking. Using commercial networks as a price efficient carrier for multi purpose communications even in technical applications is a standard philosophy in other industries. Ethernet now is broadly used in technical applications throughout many industries. Many of them even requiring soft real time behavior.[57][49]

1.6.1 Ethernet and functional safety

Ethernet as such was neither designed to be used as a functionally safe communication system nor was it intended to fulfill related standards. This imposes a number of problems when used in this context:

The CSMA/CD access method is based on a segment with collisions. Consequently, it is not possible to make any definitive statements on packet runtime. Thus, deterministic or correct sequential transmission with Ethernet cannot take place in a collision domain[49].

However, for the required failure control of a safety-related transmission, measures have to be taken, which are in conflict to the restrictions in a collision domain in the Ethernet.

The collision behavior can be minimized by using Ethernet in fully switched full duplex Ethernet environments[49].

Depending on the application, different response times and thus also corresponding safety times are required. That extends the safety requirements to the real-time capability of the Ethernet network, which today are met by use of the recent standard for Quality-of-Service.

The Ethernet timing behavior can be made "*quasi-deterministic*" by a strict load limitation of the Ethernet to about 10-13%[49]. The availability of Quality-of-Service functions in the switches and the use of Ethernet for multimedia streaming proof the today's capabilities of the technology.

Other mining applications like Ventilation and environmental data acquisition are applications where safety and a high level of communication is required. Here, response times within seconds are accepted. It must be recognized that such requirements can be implemented by Ethernet networks even with a high average network load.

Regarding all these considerations, it must be stated that it never involves a reduction or

violation of the safety requirements.

The safety-related complete system with corresponding failure control and diagnostics implements the safety function without restrictions at all times. The considerations merely involve an assessment and project planning of the system availability.

In addition to the hard requirements to meet corresponding response times, the network system has to increasingly meet the demand to transmit large amounts of data in the scope of safety-related transmission.

Thus, Ethernet generally is a suitable transmission method for this demand, which is demonstrated by numerous technical applications of Ethernet in safety critical environments. Some examples shall be mentioned here:

The industry offers a number of EN61508 certified Ethernet components as e.g. controllers and I/O units which allow use in SIL classes up to SIL3. An Internet search with the keywords "*SIL Ethernet Automation*" brings a number of related components available today from major manufacturers.

1.6.2 Criteria on safety related unified comm system

In order to enable meeting the demands of highest possible availability and thereby the potential use as part functionally safe systems first the availability criteria as outlined in chapter 1.4.3.4 have to be met.

This means to prevent from "*single point of failure*" situations by design of the communication system in relation to the mine layout (see chapter 2.1.1). Related measures are:

1. All possibilities in terms of cabling redundancy have to be used, namely ring redundancy and mesh redundancy
2. Power supply by additional independent battery backup power supplies with a autonomy time of at least 4 hrs or whatever is demanded by the regulations.

In addition, the components of the communication system have to meet highest demands on Mean Time Between Failure (MTBF) and operational availability.

If components fail in redundant setups the consequence is not directly recognizable by lack of function. If undetected or if the failure is not cured, this fact in practice leads to the system working until the backup alternative also fails and the system error becomes visible.

Therefore, the systems have to be auto-monitored and maintenance always has to be carried out without significant delay in order to assure the full functionality including the backups available at any time.

1.6.3 Comparison to traditional systems

Comparing the Ethernet communications related to the safety relevant demands as outlined in chapter 1.4.3.4 it can be concluded that Ethernet also provides the cabling robustness, if used in ring or mesh structures [20].

This fact which makes it usable in applications demanding the availability and robustness required to be used in safety-critical applications also underground.

If there is a data processing underground which makes safety related information available underground independently from above ground systems, also the processing robustness demand can be fulfilled (see chapter 2).

Criterion	Phone	LeakyF	Interkom	S-Data	Ethernet
Required by law	YES	NO	PARTLY	YES	NO
Power supply robustness	**GOOD**	**GOOD**	**GOOD**	**GOOD**	**GOOD**
Cabling robustness	**POOR**	**POOR**	**POOR**	**POOR**	**GOOD**
Processing robustness / local accessibility	**POOR**	**POOR**	**POOR**	**POOR**	**With local processing**

Table 6: Resilience of communication systems

1.7 Ethernet communication in underground mines

What started in the 1960's as a government financed research project into packet switching networks in the 1990's turned into the most widely used form of really open networking between computers[153]. Ethernet based communication today can be seen as the standardized technology for any kind of data, voice and multimedia communication. This even applies to technical communication and soft (near) real time applications for control of technical installations in industry[49].

During the early 21st century first Ethernet based systems were evaluated and introduced in mining[142]. The first mine using a fully Ethernet based communication infrastructure was the newly opened chromium mine in Kemi, Finland in 2004[142].

On behalf of a machine manufacturer the author started in 2000 to design fully Ethernet based remote service access systems for mining machines which today are available as product options even covering wireless LAN based access to the machines.

An international information exchange standard for mining machinery[114] was established from 2000 which assumes all communication to be carried out basing on the Ethernet originated TCP/IP family of protocols.

In 2003, the first coal mines in Germany were starting to establish Ethernet as networking system for use in underground mining. The first use was to enable underground workers to connect to the corporate intranet for organization of their daily work. Later also control systems were soon integrated[56].

The German coal mining company DSK also evaluated Wireless LAN successfully in 2004[5]. It's installation was in 2005 performed by the author's company within a bigger train automation project. In this context, also wireless VoIP telephony was introduced in coal mining.

Today, the focus is on integrating the technologies in order to unify communication on Ethernet and WLAN in order to cost efficiently enable process optimized mining operations.

The established technical setup is a hard wired backbone infrastructure using Single Mode optical fiber. For cost efficiency, multiple active units are daisy chained in a ring structure, where two different shafts are used to bring the data to above ground. The ring is closed above ground or on a different mining level underground. The active units along the chain mostly are equipped with Wireless LAN access points providing wireless coverage in the area around them.

2 SAFETY SUPPORT FOR MINE COMMUNICATIONS

This section describes the mine safety related functions for underground network communication, as they were designed within the work subject to this thesis. Key functions for this are also subject to an international patent application as filed as one of the results of the works for this thesis under [115]. This chapter describes the possible functions related to a Safety Support Communication System, while chapters 3 and 4 describe the implementation of important parts of those.

2.1 Extended Ethernet Functionality

This chapter describes all Ethernet based functionality, which is used to derive mine safety related functionality from.

2.1.1 Mine layout versus communication system layout

An underground mine consists of a network of tunnels (chapter 1.1.1) which today can be represented graphically in a model vectors ("*tunnels*") and nodes ("*crossings*") as explained in chapter 1.1.3.

If the tunnels are equipped with network cables (or Radio Frequency wireless links) and active network nodes are placed at the crossings, the resulting network structure represents the physical structure of the underground mine. This representation however is limited to the subset of those tunnels equipped with communication links[125][115].

If the status of all network links and nodes is reported to a mine visualization software above ground[54], the status of each link is directly visible in real time on a graphics screen[20]. Furthermore, this information can be processed in order to derive safety-relevant information from it (see chapter 2.3).

An important precondition for such an architecture is the choice of the "*right*" communication system. As discussed in chapter 1.4, the architecture of most traditional communication systems only allows an application in line and star structures, which do not match the mesh like structure of an underground mining environment.

However, these demands can be met by Ethernet based communications in a way that the passive components (fiber or copper cables or even a Radio Frequency Link) are routed through the tunnels, while active components like switches are placed where the network links and thereby also the tunnels meet: At tunnel crossings.

This principle makes three elementary components match:

1. The physical tunnel layout
2. which is fully or partly represented by the communication links and switches
3. whereas 1) and 2) are visible on an above ground graphic visualization using a true 3D model of the mine layout

2.1.2 Function overview

In order to enable the network to be part of the underground safety, the communication system as such needs to be resilient in a way, that foreseeable failures do not lead to a failure of the complete system[20] [19] [16] [98]. This means that the network has to be robust against the potential failures as analyzed in chapter 1.4.3 and 1.6.3:

1. Loss of supply voltage for the active parts of the system
2. Cable failures
3. Resilience of data processing and availability of central services

While the first functional demand is covered by standard battery backup power supplies, the demands on cabling redundancy and functional and logical resilience require substantial research outlined in the following chapters:

2.1.3 Cabling redundancy

Ethernet as such in accordance to the IEEE 802.3 BaseT or BaseF as used today are set up using direct connections between two network participants in form of switched networks [49], [153], [61]. This also is the setup for underground networks, where mainly fiber optic cable is used [56]. In order to prevent from all cables being routed to central switches individually, the switches are daisy-chained on a high bandwidth line enabling network clients to hook up to the broadband network at these intermediate switches (figure 2).

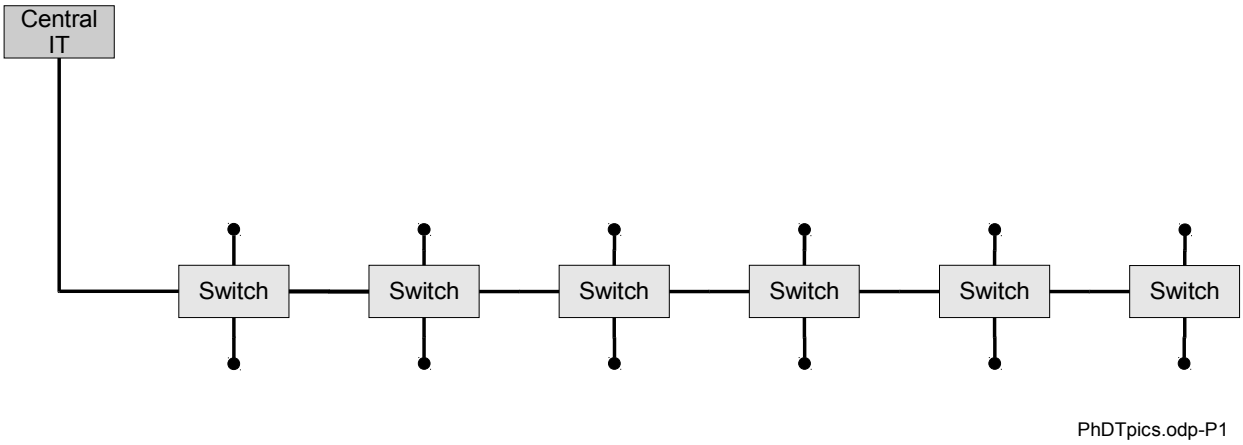


Figure 2: Daisy chained network line

This setup however makes the functionality of the connected devices salvageable when one of the switches fails or one of the communication links between the client and the Central IT collapses. This failure would leave all infrastructure behind the failure out of function [110]

[115].

The first extension to this architecture is to set up the network hardware in a ring structure as shown in figure 3. This layout provides a one-failure safety: One component (cable or switch) may be out of function while all other components remain working [133],[56],[115].

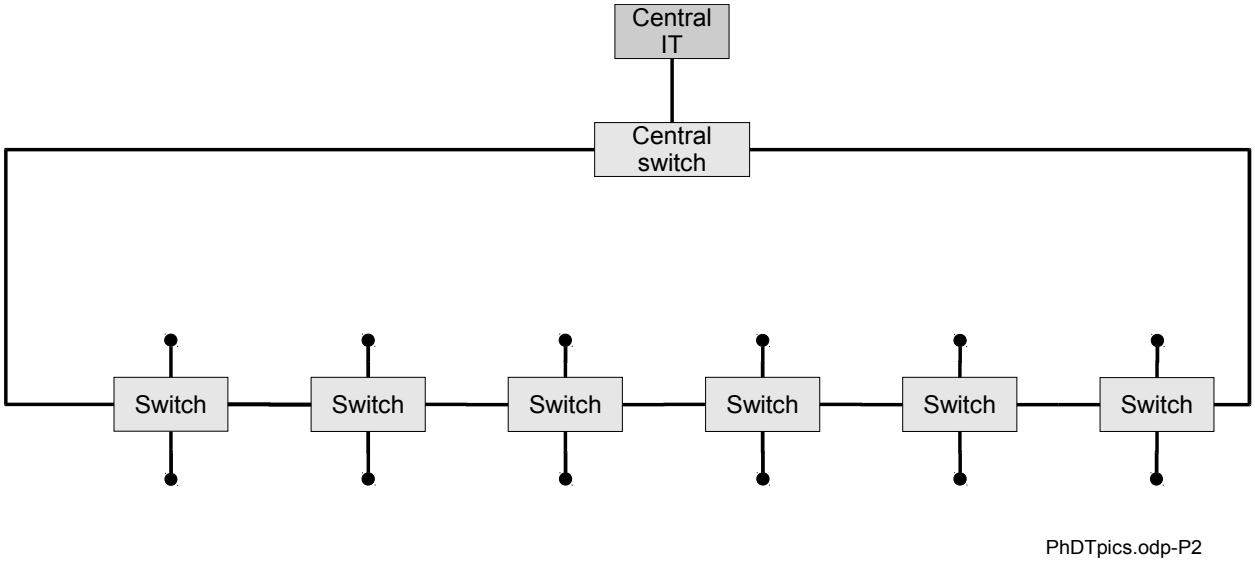


Figure 3: Network layout in a ring structure

Running ring topologies in Ethernet means that the access to the communication media has to be controlled in order to prevent from multiple paths from one endpoint to another being active at the same time. For the creation and operation of redundant ring topologies different proprietary methods are available [148],[1],[37], which mostly are supplier specific. These are not taken into account for this thesis, as it was the goal to create a system basing on open standard technologies.

Today, standardized methods like the "*Rapid Spanning Tree Protocol (RSTP)*" acc. to IEEE 802.1D are available to manage and operate Ethernet ring topologies and thereby to prevent from multi path situations. Such functionality is to be used at least for the central switch in figure 3. The other switches in the ring may be passive as they do not need to actively open or close one of their backbone ports. These switches just have to allow the administrative RSTP network packets to flow through. These "*Bridge Protocol Data Unit*" (BPDU) telegrams are exchanged in the network in order to detect loops and to organize how loops are cut and which ports are to be used [60].

Assumed that the switches in figure 3 are located underground and the central switch is located above ground, the central switch connections can (and preferably should) be routed to

above ground using two separate exits of the mine (shafts). Thereby a highest possible resilience in this ring structure can be achieved [16],[115],[110].

In case that two components in this ring structure fail, multiple network components or whole parts of the infrastructure are out of function as they will not have an operative connection to the central switch any longer. In this case the fact that a mine is a graph of meshed tunnels is helpful: Additional cables routed through the tunnels interconnecting two rings (green dotted lines in Figure 4) help to increase the cabling resilience of the complete installation [115].

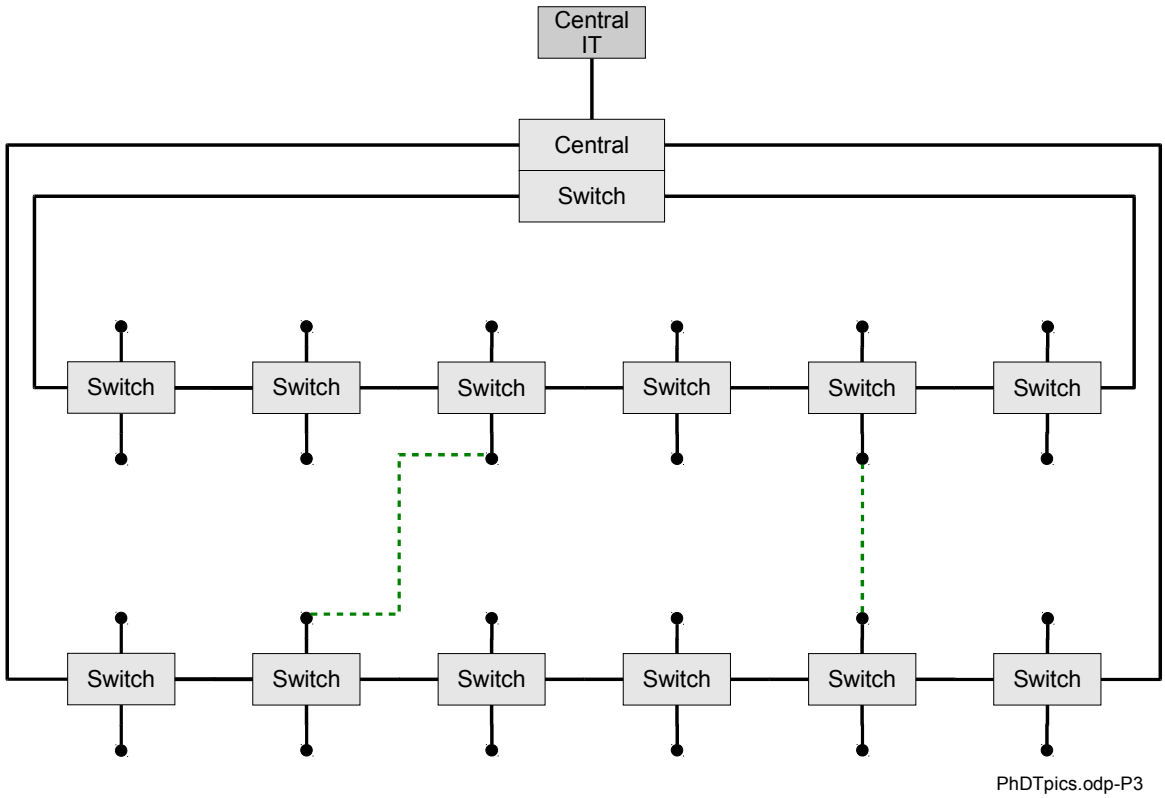


Figure 4: Rings with redundancy connections

Now, also the switches connected to the redundancy connections (dotted lines in picture 4) have to be capable of actively managing RSTP functions, meaning that they have to be able to open / close all connected ports with active RSTP traffic.

However, as explained later in chapter 3, the capabilities of RSTP are limited due to some protocol immanent limitations. Nevertheless it is a usable standard procedure to assure a highest possible underground network cabling resilience at a reasonable cost.

2.1.4 Regular operation mode and emergency mode

For the operation of an Ethernet network, central services are needed. The most basic

service is the "*Dynamic Host Configuration Protocol*" ("*DHCP*") [165], which dynamically assigns the IP addresses to the attaching client computers or network devices.

Other services include the "*Session Initiation Protocol*" ("*SIP*") in accordance to RFC 3261 [166], which allows to establish Voice over IP ("*VoIP*") connections for phone (voice) communication in a network.

These and further central services usually are provided by central servers located in office buildings above ground. Due to the nature of these services it is understandable that these services need to be maintained even in a case, when all cabling redundancy fails and big parts of the underground networks are disconnected from above ground central systems.

In such case, the resilience of the data processing and the availability of central services becomes crucial as well as communication in any case of hazard be it an above ground earth quake or an underground fire is essential for surviving and efficient search and rescue operations.

2.1.5 Maintaining services upon connection loss to central services

In a case when all communication to above ground is lost, which automatically means that all hardware redundancy has failed, the underground network hardware will still be functional as it can be assumed that whatever hazard happens it will never in a single sudden event harm the entire mine at the same point of time. However due to the connection loss to above ground, the central services will be disconnected resulting in the fact that the underground communication would be physically possible because all hardware is running, but it is disabled because the access to the central servers is out of order resulting in a physically available but unusable network [115][16][19][20].

Therefore, a major part of the safety related network communication system presented here is the functionality of keeping essential network services alive when the connections to above ground are lost [115] [124].

In a physically resilient network this situation as such is so unusual that it's occurrence can be interpreted as an emergency situation [20]. Therefore, the availability of the connection to above ground servers is a basic criteria to decide upon the operation mode of the active underground network components [115][124][123]

- Servers available = Regular Operation Mode
- Servers unavailable = Emergency Operation Mode

Following this rule, every single network node has to be able by itself to determine about this status. Consequently, the smallest possible disconnected network - "*island*" in the underground network is one single network node and due to the fact that the kind and extension of an emergency cannot be predicted, the software for all basic network services has to be available on all active network nodes [115]. As this software is not used in Regular Operation Mode, it can be activated in Emergency Mode if needed.

When a network island consisting of 1-n network nodes is disconnected, the nodes in this network island negotiate among each other, which node has to provide a certain central function. It is important that the services are distributed on several nodes in order to prevent from performance problems. The way how this negotiation is performed is described in detail in the Implementation Chapter 3 below. After these negotiations are performed and the services are started, the network is running in an Emergency Mode. In this mode, the network functionality is limited to basic services like voice communication, tracking of people ("*who is where*"), distribution of environmental data and other special emergency case functions described in chapter 2.3 below.

2.2 The Network as distributed Safety Support Computer

In order to make the network independent from any above ground server connections support the miners in case of an emergency, the active computing components in the network need to have all safety related location based information stored on the devices. Further information shall be obtained from other safety related systems working in a mine like e.g. the environmental monitoring or gas sensing systems. In case of an emergency, all this information is used for the functions explained in the following sections of this chapter. A brief overview also is available in [113]. The most important functions are:

1. Help to electronically locate an emergency inside the mine
2. Provide information about locations of safety equipment
3. Locate people underground
4. Help to guide people to safe locations

For these purposes the Network nodes store and process the following information:

2.2.1 Static infrastructure information in the active network nodes

A precondition for using network status information in a location based context is that the basic infrastructure of at least a part of the mine is known to each network node. Therefore, every node has to have basic information available about the mine's tunnel layout [115]. This "*tunnel map*" is comparable to the map information in a road navigation system providing the street map in a car's navigation computer. In this graph, a tunnel crossing or intersection of tunnels is represented by a node while each tunnel is represented by a vector which also includes length information and additional properties like whether or not this tunnel is passable for people. This means that a complete static tunnel graph is available for any location based computations.

2.2.2 Network hardware overlay

As an overlay to this static tunnel graph, the network's hardware layout is downloaded. As mostly not all tunnels are equipped with network cables and as network cables only can be routed through tunnels present in the static map, the network hardware overlay will conform a subset of the static tunnel graph, namely those tunnels with network cables routed through. This overlay also contains information about the locations of network nodes and the routing of cables in relation to the mine's tunnel graph.

2.2.3 Safety Equipment Overlay

A second overlay to the static tunnel map contains all locations of safety relevant equipment [124][125]. In this overlay map the locations of all items are shown which can be of importance to support underground safety like:

1. Exits and emergency exits
2. Rescue chambers
3. Fire fighting equipment
4. First aid equipment
5. Environmental sensors

2.2.4 Access to environmental information in the underground network

The locations of environmental sensors are known from the Safety Equipment Overlay map. In order to use the information from such sensors, the sensor data has to be available within the network. Due to the fact that (at least in coal mining) today all environmental sensor communication is based on serial (telephone communication based) cables, this function needs interfaces to such environmental or gas monitoring systems underground[122].

Such interface can e.g. be a serial link between the network nodes and environmental controllers. Ideally, especially in new mining installations, a direct Ethernet interface on the environmental controllers should be preferred.

In addition, the environmental monitoring system needs to process the sensor information in distributed controllers underground. This is a lack in most today's installations as in many cases the raw data is communicated to above ground and all data conversion and interpretation takes place above ground. In this matter a philosophy change is needed in order to make environmental information usable for direct underground Safety Support Systems.

2.3 Network Related Safety Functions

Presumed that the network after an underground emergency is at least partly usable underground (see previous chapter), it can work as a safety support system providing a number of functions which can conform a crucial support for quick and structured response to the situation and help both the people underground and also external rescue teams entering the hazard zone.

As soon as the Emergency Mode is started, the network infrastructure immanent safety support functions explained in this chapter are run in order to have all this information available to be communicated to the workers as soon as needed.

2.3.1 Determining network structure and Link status

A precondition for each network node to interpret network information in a location based context is the knowledge of the locations as derived from the static tunnel layout (chapter 2.2.1) and the real time network status information (Figure 5).

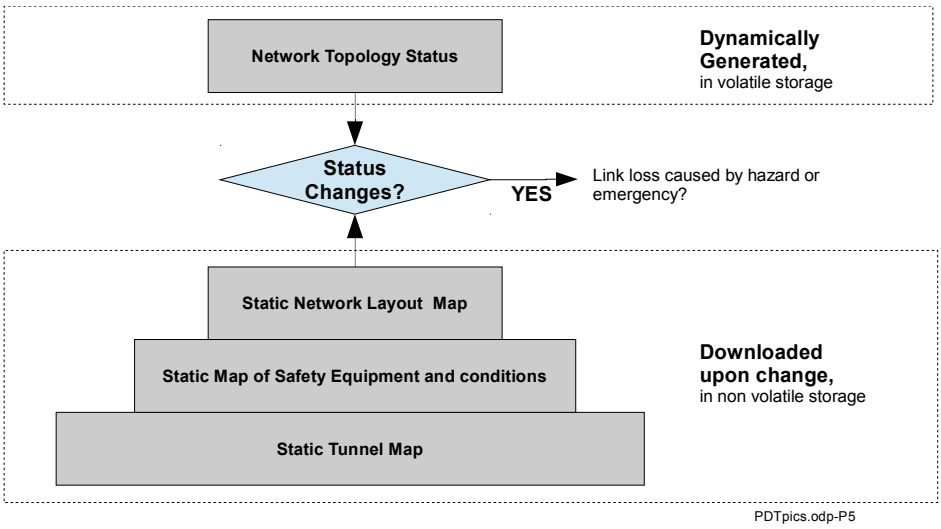


Figure 5: Network Status and Tunnel Maps

During operation, all network nodes exchange administrative telegrams in order to keep track of each others status, the status of the links between them and the status of the links to the above ground servers. This way, the status of the entire network is independently known to every single network node in the system [115]. As each node is able to compare this information with the downloaded static network map containing the cabling as it is installed, changes in network operation and link status can be detected and interpreted for guidance applications or safety support[122].

2.3.2 The network as mine wide safety sensor

In case of an emergency underground it is often hard to determine, where exactly the accident happened or started. As the network links (cables) routed through a subset of the tunnels, the status of the related communication links running through the cables (and thereby through the tunnels) can be used as part of an intelligent "*sensor*" for an emergency [125].

From a network link status sensing the following can be derived as safety information to localize an emergency:

1. A working link inside a human passable tunnel or shaft can be interpreted as the related tunnel which the cable is passing through is most probably also passable for humans. Related tunnels therefore most probably are available for an evacuation [115].
2. A transition from a working link to a lost link in conjunction with a link loss to above ground or another declaration of the Emergency Mode may be electronically interpreted by the network nodes as as potential area where the accident or hazard happened. This in turn results in a strong probability that the tunnels the cables are routed through may not be passable for humans any longer.

In these situations, only the interpretations above are allowed, reverse conclusions are not valid!

2.3.3 Securing Link Status interpretation by Additional Data

Not every single link loss may be interpreted as an emergency: Mining practice is so dynamic that often power is switched off, cables are re-routed or temporarily unmounted due to e.g. heavy equipment transports etc. Thus, a link loss condition should only be firmly interpreted as caused by a mine emergency in conjunction with additional information which should be available locally in the network without involving above ground systems as e.g.:

1. A person triggers any kind of safety alarm (e.g. fire alarm)
2. Environmental sensors for ventilation parameters like barometric pressure, air speed and air flow direction as well as air temperature
3. Data from fire detection and alarm system including the related location information
4. Gas sensors for burning gases like CO or smoke particle sensors
5. Gas sensors for toxic and / or flammable gases

This additional data may be available only with some time delay to the network breakdown which occurred before depending on how far the related environmental sensors are located from the occurrence and the network breakdown point. In other cases, the gas sensing can also be prior to the network link breakdown, so a time window has to be set for interpretation[125].

Again it shall be emphasized that for all such conclusions basing on multiple information sources – whereof the network structure is one, the integration of the information in distributed underground intelligent systems is essential to make it available not only on above ground servers but also in the network underground [115], [120].

Normally today, all such sensor information usually is collected and interpreted in separate data collection and automation systems, which in turn are not necessarily connected to an Ethernet network underground. For a full functionality of the Safety Support Network, these systems have to be interconnected with the intelligent network nodes and also these systems need to make use of local, distributed intelligence underground which enables the propagation of the related information in the underground network even during connection loss to central systems.

2.3.4 Hazard Location Detection

Under these circumstances, a link loss can be interpreted as an emergency as follows:

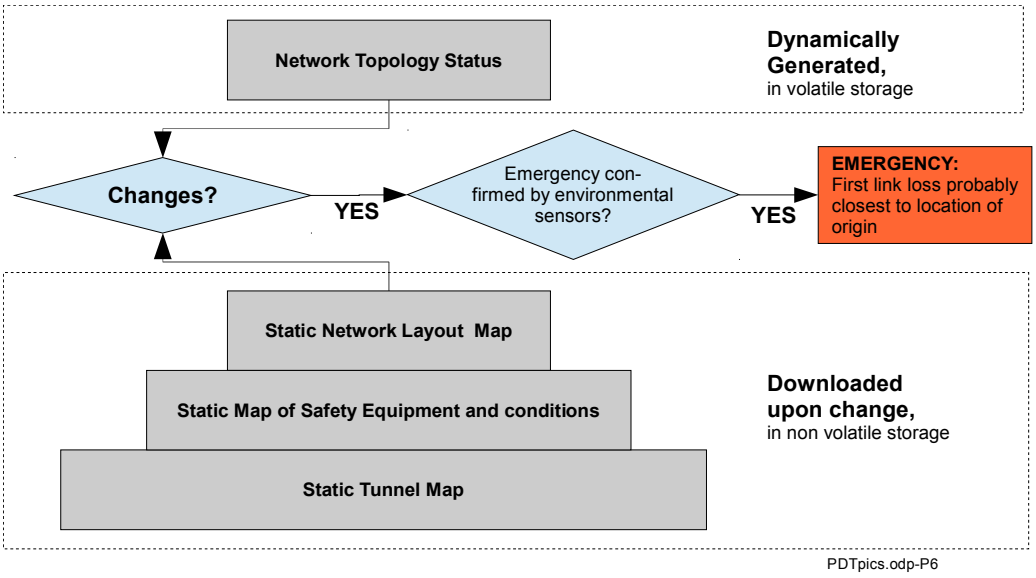


Figure 6: Hazard detection from link loss, maps and environmental sensors

If the changes in the actual network topology status are confirmed by additional

information and / or a human triggered Emergency call, the first link loss most probably can be determined as having occurred closest to the actual hazard. This interpretation is valid for all emergencies which cause an destructive impact on cables and / or electronics like rockbursts or fires, which is explained by two related examples:

During a rockburst (earthquake underground), the event is always first detected by seismic accelerometers nearly at the time of event occurrence (t_0). If the rockburst causes tunnels to collapse, the lost network links (t_{LL}) will be the second event to be detected. If a tunnel completely collapsed, this also has to cause changes in the underground airflow, so the last will be changes in ventilation air flow which are to be seen at t_{VC}.

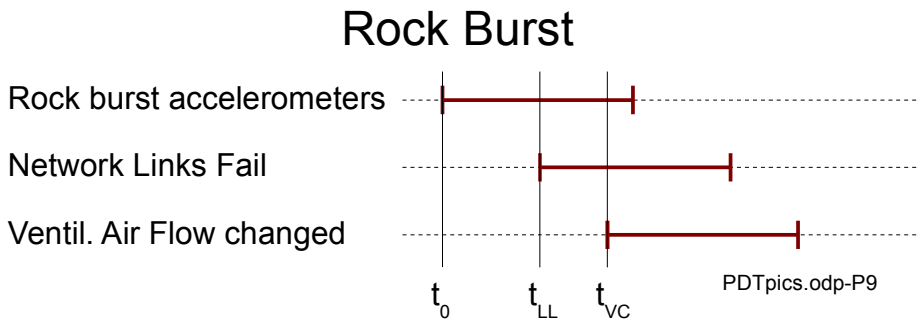


Figure 7: Typical event timing during a rockburst

The outbreak of the fire may be sensed first by network links breaking down at t_{LL} due to either fire and thermal damages to the active electronic equipment or similar impact on fiber optic cables. This will finally be followed by the detection of burning gases which however can take some time, which is determined by the air speed and air flow direction in the related area, because a gas sensor has to be triggered which is located in the downstream of the airflow seen from the event location. Especially in a fire case, determining the hazard location via the network infrastructure therefore is the most accurate and price efficient method.

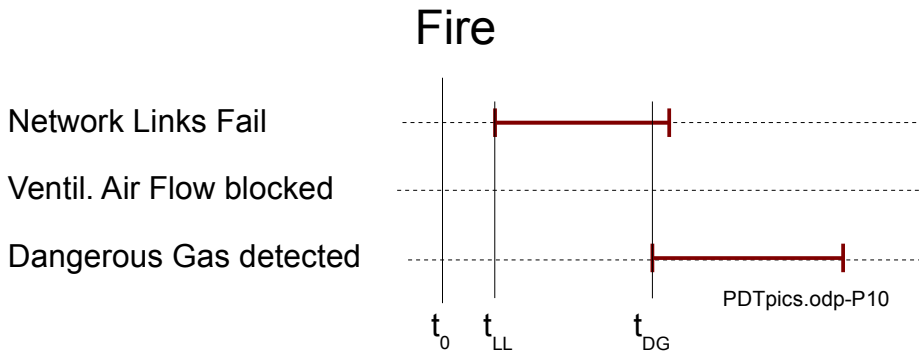


Figure 8: Typical event timing during a fire

In any case a correct interpretation of a link status or it's transition requires to mask out erroneous alarms. Therefore, maintenance work in the network has to be announced in advance and downloaded to the network nodes together with the Static Network Maps so the probability is minimized that an operational link loss is being interpreted as Emergency.

2.3.5 Link Status for „Emergency Exit Available“ Indication

In the same way a link status is interpreted as sensor for hazard detection, the network status also helps in finding an emergency exit available for a potential evacuation of the workers following an emergency[115].

The procedure uses the same basic data as the hazard detection scenario: The network nodes use their real time network topology status information overlay-ed onto the static mine map supplemented with the locations of safety equipment to determine where potential exits could be accessible.

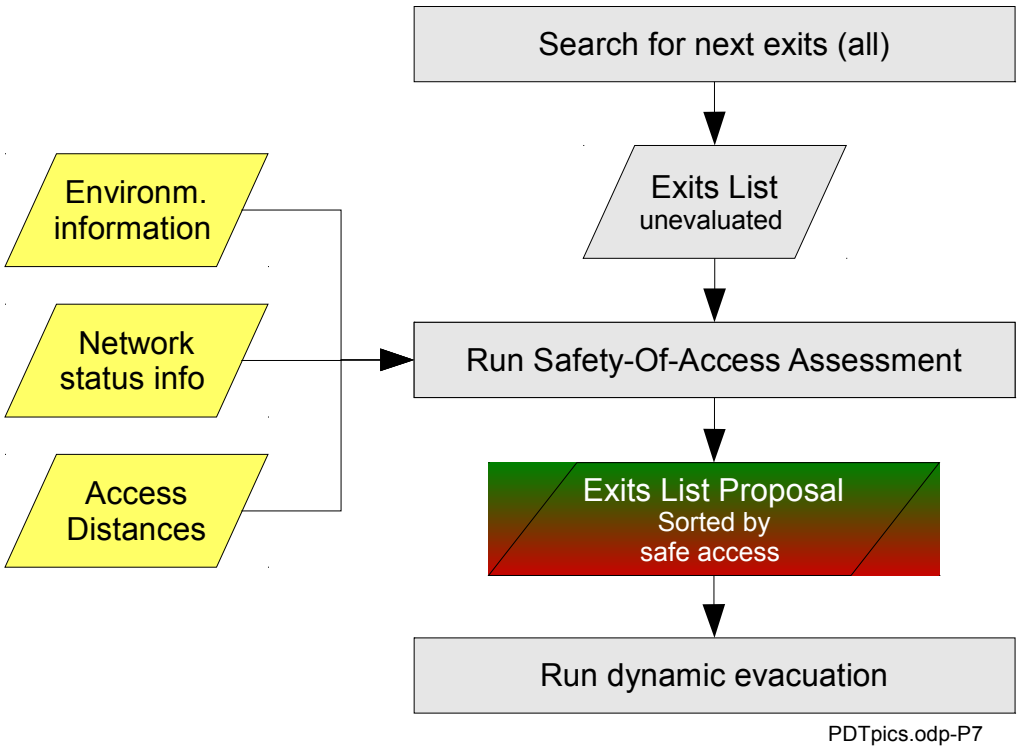


Figure 9: Emergency Exit evaluation process

The general procedure starts in the Network Node with searching for all exits available in the area. For this the Network Node uses the Static Mine Map together with the static Safety Equipment Overlay.

The result is a raw list of all exits in the area or beyond. However this list does not take into account the actual situation in terms of which of the exits really is accessible.

In a second processing step, the Network Node runs a Safety-Of-Access Assessment. The goal of this assessment is to produce a list of emergency exists sorted by their accessibility under the actual conditions of the special safety case. This may result in the fact, that it is safer to propose an exit further away which is accessible without dangerous gases in the tunnels rather than an exit close by where burning gases were sensed. The method of this evaluation is to compute a "*routing*" from the network node to the exits and rank the routed to one or more exits according to the results of the Safety-Of-Access assessment resulting in a list with the most probably safest exit route in the top and the more dangerous routes in the bottom in order to present this list e.g. on displays of the network nodes or on WLAN connected personal devices of the miners [124].

This Safety-Of-Access assessment uses the link status interpretation from the hazard detection procedure (see 2.3.4) together with environmental and ventilation information to determine whether or not the routes to the exits are most probably passable for humans. This procedure shall be explained in detail:

For determination whether a tunnel may be used for an evacuation, table 7 shows the status of network cabling and ventilation information and the results whether or not a tunnel may be passed in these conditions.

The regular condition today is case No. 9 in which neither network information nor ventilation data is available to the people underground. The consequence is, that they have to personally evaluate whether or not a tunnel can be used for evacuation. In an emergency situation with raising temperature, lack of fresh air and potentially dangerous gases around, this procedure can be dangerous to the health of people involved. It is also a very time consuming procedure which eventually also may lead to fatalities as the lifetime of catalytic air filters is limited to a couple of hours. Consequently, any improvement of this situation helps to save life.

Limiting the interpretation of table 7 to the availability of network cabling, the transition of an available link (case No. 3) to the same link suddenly breaking down (case No. 6) is relevant for the most cases, because only a minority of tunnels is directly equipped with air flow sensors. The result is that the working network cable is interpreted as "*Nothing happened to this tunnel"* which means that it most probable still is passable for humans. When a link is lost, this

will be interpreted as the tunnel most probably is not passable any more (case No 6). This interpretation can only be proven invalid when a ventilation air flow is positively sensed for this particular tunnel.

	Network Cable installed and working			Network Cable installed but NOT working			No Network Cable installed		
	Normal with sensors	Tunnel pot. Corrupted but Cable working	Normal w/o vent sensing	NW cable off; Vent OK	NW and Vent off	NW not working, no vent data	No WN data, vent working	No NW data. Vent not available	Normal today: No info
Case No	1	2	3	4	5	6	7	8	9
Network Cable working	Y	Y	Y	N	N	N	na	na	na
Ventilation Flow through tunnel	Y	N	na	Y	N	na	Y	N	na
Result, advise	**S**	**NP**	**S**	**S**	**NP**	**NP**	**S**	**NP**	**EP**

Status explanation	
Positively sensed safe	Y
„Unsafe“ reported by sensors	N
No sensors / data available	na

Result Codes	
Passable	**S**
Evaluate passability	**EP**
Probably not passable	**NP**

Table 7: Network Link Status and Passability of Tunnels

This leads to the following rules for the Safety-Of-Access assignment:

1. A tunnel which is marked “*passable for people*” in the static tunnel properties with a functional network cable inside is regarded physically passable for humans (Cases 1-3).
2. The tunnel which is marked “*passable for people*” in the static tunnel properties according to cases No. 2, 5 and 8 is regarded verified physically impassable for humans when the tunnel shows no airflow sensed by a ventilation sensor installed in this tunnel, while it showed air flow before.
3. A tunnel which is marked “*passable for people*” in the static tunnel properties with a ventilation sensor installed in this tunnel is regarded verified physically passable for

humans when the tunnel airflow sensor shows an active airflow (cases No. 1, 4 and 7).

4. A tunnel which is marked "*passable for people*" in the static tunnel properties with a network cable status transition changed from "*available*" to "*unavailable*" in conjunction with an emergency situation, is regarded probably impassable for humans (valid for cases No 5 and 6).
5. All other tunnels – which most probably are not equipped with network cables – are shown with unknown status, meaning that the passability has to be evaluated, unless a ventilation sensor is installed and data from this sensor is available.

While the physical passability of a tunnel is the primary criterion for a possible evacuation, the presence of dangerous gases is an important additional information which may impact the health of the evacuating people. Even when they are using e.g. catalytic filters to generate breathable air, their physical condition may be impacted by this situation and such evacuation should be avoided if safer alternatives are available. Therefore a full implementation of the Safety Support system has to take this into account by integration of the environmental sensor information available.

The goal of this optimization is that each passable route is assigned an environmental safety information stating the information of the gas sensors available in the network.

As a precondition for these functions, the Safety Equipment Overlay (2.2.3) map has to specify the emergency exits at their respective locations, which is stored in the individual network nodes.

To identify an available exit the network nodes inside a disconnected island run the following procedure:

1. In the Safety Overlay map search for the nearest regular or emergency exit.
2. The network node determines a proposal of how to reach this exit by taking into account the distance and the environmental information about the area in order to assure that the exit can be reached safely.

Basing on this data each network node is able to provide situation dependent information about possible emergency exits (*Exit List Proposal)*. In case multiple options exist, the network nodes creates a ranking of the exits basing on additional information available (e.g. from gas sensors) in order to avoid guiding people into an area contaminated with poisonous gas when an

alternative exit is available in a better environment.

The result is a List of available Emergency Exits which is ranked by the safety of their accessibility and which contains the following information for each emergency exit:

1. Name of the Exit
2. Position
3. Distance from the current network node
4. Safety tag

In this list position 5 states a safety tag which expresses the accessibility of the exit basing on the environmental sensor information available en route to the exit:

1. SAFE (green) meaning that the route is to be safe which has been positively confirmed by environmental sensors en route in combination with a confirmed fresh air flow e.g. from this exit shaft into the area where the people are present.
2. UNKNOWN (yellow) meaning that not all area can be confirmed safe by environmental sensors. So increased care is needed when using these routes, potentially they are only passable using breathing filters.
3. UNSAFE (red) meaning that at least one environmental sensor en route has actively detected an unsafe condition (e.g. burning gases, smoke etc)

For distribution of this information Displays at the network nodes can be used as well as personal wireless communication clients worn by the staff.

After an exit has been found, a dynamic evacuation procedure in accordance to chapter 2.4.2 may be initiated.

2.4 Location Based Safety Support Functions

This chapter describes all Safety Support Functions derived from network immanent information or from a combination of network status and environmental monitoring information.

2.4.1 Tracking of People

Tracking means that the locations of people or assets are stored together with a time stamp when the person or asset was electronically recognized at a particular location. Such demands already have been made mandatory by particular legislation [164]. In contrast to traditional systems, the network nodes proposed in this thesis do not only forward tracking information to servers above ground, but they also generate tracking information from wireless LAN clients or other connected tracking systems (e.g. RFID based) and store it locally. This has two decisive advantages for supporting underground safety:

1. The information "*who is where*" is available on the network nodes and thereby available for further going interpretation in dynamic evacuation (2.4.2) or to report to SAR teams whether an area is already evacuated (2.4.3).
2. Underground workers can determine locally whether or not other people are in proximity around themselves.

In traditional systems as installed today, the tracking information again is available on central servers above ground exclusively. This may be good to direct SAR operations from outside, but it does not help the workers underground in case of an emergency. Furthermore, this information available above ground is always outdated when a communication breakdown occurs as it cannot be anticipated that the people underground in an emergency will stay where they were at the time the emergency occurred.

As it cannot be assumed that tracking devices from only one single supplier are to be used and all personnel related tracking data needs to be integrated to make the system working, the use of devices using standardized tracking information exchange should be preferred. For details see the implementation chapters.

In the new Safety Support Network, the tracking information is generated by each WLAN equipped Network Node from the data of associated WLAN clients. This means that every person equipped with any WLAN device automatically is tracked by the Network Nodes [115].

The Network Node stores this information locally. Only when the person is positively

reported associated to another WLAN Network Node, the information is marked outdated in the previous node. This procedure assures that a person always is registered in one node, even if he moves out of WLAN coverage.

When Emergency Mode is triggered, all tracking information in the Network Nodes has to be "*frozen*" by storing it to non volatile memory in order to be able to reproduce the situation at the time of an emergency.

In the same way the tracking information is stored again to non volatile memory shortly before the Network Node runs out of battery power in order to store the situation before the unit shut down. This enables SAR teams to evaluate the situation when they reach the node later and power it up in order to see whether or not people were reported in this area when the node shut down[115][16].

2.4.2 Dynamic evacuation

Basing on the tracking information together with the static mine map and the overlays for network structure and Safety Equipment the network is able to help the miners in an Emergency to behave in the safest possible way and possibly also to find a safe to use emergency exit [16] [115].

This network supported dynamic self escape covers three stages:

1. Decision Making phase
2. Meet either all together or in groups in different locations in the "*Mustering*" phase.
3. Evacuate in groups

2.4.2.1 Decision making

In the Decision Making phase, the people communicate with each other their opinion on the situation and the situation will be finally assessed with the conclusion of what to do. In this phase, the network supports the use of wired and wireless IP phones by enabling a Voice-over-IP communication by providing the related central SIP services in the network nodes.

In this phase, the proposals for evacuation routes as explained in chapter 2.3.5 are evaluated either on mobile computing devices or by looking on the network node screens.

Finally, a procedure is agreed. This may be that different groups are trying to meet in

different locations or all people meet in one single location.

One person then declares this decision for the meeting point(s) via his mobile computing terminal to the network nodes or the person closest to the meeting point node pushes a button at this node. This is to make sure the network nodes know about the meeting point in order to be able to activate guiding functions for the miners approaching the meeting point in accordance to the next chapter.

2.4.2.2 Mustering

Now, all miners are walking to the agreed meeting points. In this situation it is important to assure that nobody is left behind. This is supported by the network's tracking functions (2.4.1) [115]:

Provided that all people are equipped with man tags or mobile WLAN devices, each network node knows that persons were reported in it's proximity. When now all people move towards the meeting point, they have to pass from the coverage area of one network node to the next, even if the coverage area of the "*next*" network node is not directly connected to the coverage area of the previous one. This means that the new network node upon connection of a client has to inform the adjacent network nodes in order to enable the previous node to delete the man tag or network client from his list of tracked devices. This makes all WLAN clients and man tags to be registered with the last network node they were attached to, even if they moved into a non covered area beyond the network node's coverage (see chapter 2.4.1).

Is the tracking list of one network node empty, so is this interpreted as "*there are no people left inside this area*". Through the declaration of the meeting point(s) the network nodes also know the moving direction of the people which enables them to declare visually on their displays or via the WLAN "*There are no people left behind*" in the area of the network node and towards the outer leaves of the network [115].

This positive evacuation information is stored in permanent memory on each network node to make this information visible to SAR teams entering the mine later after the network nodes have run out of power (see chapter 2.4.3).

When all people have met up at the agreed meeting point, they may later decide to make an attempt for self-escape.

2.4.2.3 Network supported self escape

For self-escape the group chooses a route from the list created by the network node in accordance to the procedures in chapter 2.3.5. In the meantime, the safety situation may have changed, so they will look on an update of the proposal tables and combine the safety support information they get from the network nodes with their own observations and impressions and make a decision on which route to choose and whether or not to use the safety support information from the network.

If the people choose to follow a self escape route as proposed by the network nodes, they also can be guided by the network nodes. The network nodes also can give them electronic guidance via their mobile data terminals or as a picture on the network node displays.

Also in this case, the nodes keep track of WLAN clients in their coverage area and store the "*no device left in area and behind*" information in permanent memory for possible later access [115][20].

2.4.3 Support of external Search and Rescue (SAR)

External Search-and-Rescue defines the operations initiated by the people above ground or in areas of the mine not affected by the Emergency. Every mine has to have specially trained Mine Rescue teams, which in case of an Emergency have the tasks of responding to the individual situation and especially to save and rescue life. These teams are entering the dangerous areas as soon after an emergency as reasonably possible at a calculable risk for the rescue team [126] [77] [79].

In an Emergency two diverging operational situations arise right after the loss of all communication: The isolated group(s) of people underground on one side which perform own actions to leave the dangerous areas and the operations of the SAR teams. The SAR teams have to find the people underground as soon as possible in order to be able to assist and to save lives. This has been demonstrated impressively by many mining accidents and even by spectacular rescue operations like the latest in Chile in 2010 [173].

2.4.3.1 Situation evaluation support

In such situation the actions taken above ground have to be basing on the information available just prior to the event, which puts a high emphasis on knowing where the people were

right prior to the emergency. This in turn is given by the tracking functions as described in chapter 2.4.1 and the storage of all tracking information in a historic database (chapter 2.5), so this information can be accessed before rescue teams start actually working.

Similar information has to be available for all the environmental and ventilation situation underground, which is a standard data acquisition in most mines today with the difference, that this information mostly is not communicated via networks but only via telephone wire based data acquisition systems – at least in coal mines.

This information is used by the rescue teams to evaluate the situation and to predict where survivors potentially can be found and how to get access to them. An important question in this respect is the prediction of what people underground will most probably do as they now are fully on their own.

Getting access to this information as soon as possible after an Emergency can be of crucial importance for the rescue teams in order to provide fast first aid and to not expose the rescue teams to unnecessary risk of their own life.

2.4.3.2 Mobile SAR network and temporary network repair

For this purpose, the Safety Support network includes the possibility for setting up a mobile temporary network between the rescue team and a rescue base underground which normally acts as an on site operation center.

This mobile SAR network consists of a mobile cable drum of fiber optic cable [115], which in it's core hosts a built in network node of similar type like those installed in the mine normally. When the rescue team processes, this cable drum is rolled out leaving the cable on the tunnel floor. When the end of the cable on the drum is reached, a new drum is rolled out and the network nodes inside the drum core powered by batteries provide wireless access functions for the members of the rescue team [115] [16].

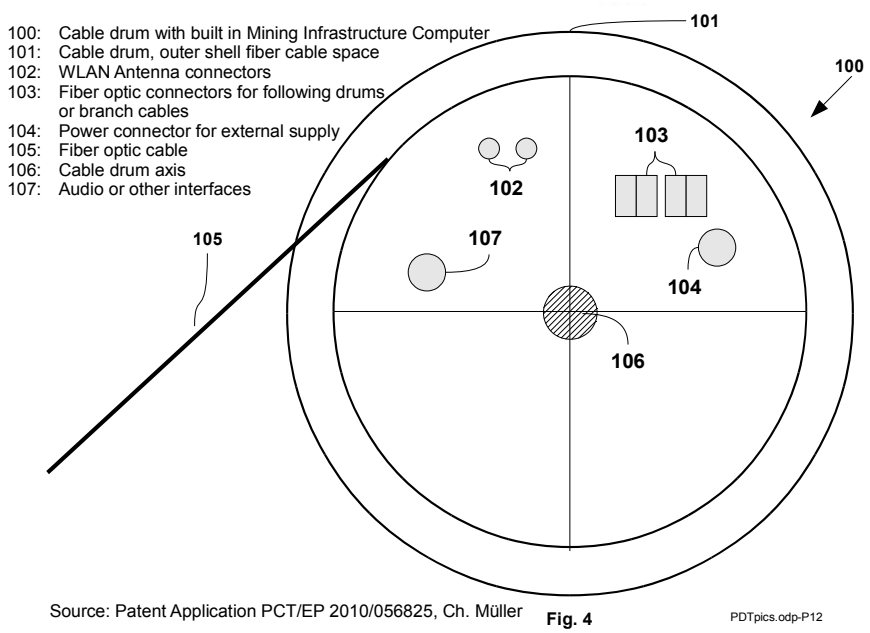


Figure 10: Core of cable drum with built in network node connectors [115]

This mobile SAR network is also of importance when the rescue teams enter the area which formerly was disconnected: By connecting the mobile SAR network to one formerly disconnected network node the rescue teams can access two different important functions:

1. The evaluation of the tracking information from the formerly disconnected network in order to allow the SAR team to direct further activities
2. If the network is not out of power yet, the SAR team gets the possibility to communicate to the people in the formerly disconnected area.

2.4.3.3 SAR team access to tracking information

In case the network in the disconnected area is still alive upon a SAR team connecting to it with the mobile equipment, all person tracking data can be read out directly from the network nodes, giving a full overview of the locations of the people underground at this moment.

In case the network was already down due to battery low situations of the active network nodes, the first node is powered by the SAR team using temporary batteries. In this case the tracking information stored in permanent memory can be retrieved from this unit as far as available until the connections dropped out due to the active network nodes one after the other were loosing battery power.

This analysis is done by the operation center while the SAR team can continue its work.

The team will then be directed in accordance to the tracking information received from the network node in order to fastest possible get to the people in the emergency area.

2.4.3.4 Audio communication with safety headsets

During an underground emergency, rescue teams are using breathing apparatus which disable them from voice communication to a big extend. Therefore, microphones and loudspeakers are integrated into the standard breathing masks to be connected to radio communication handsets for rescue team communication[31].

If the Network Nodes are equipped with VoIP units [15] to enable voice communication via the network, an additional connector for those headsets can be used by rescue team members to try to communicate with the trapped people as far as the active components in the area still area alive.

Picture 3: Protection Mask with integrated communications (Draeger) [31]

When a rescue team member enters into a formerly disconnected area with network nodes still active, he disconnects his headset from his team radio and connects it with the VoIP plug on the network node in order to try to communicate to the people inside the formerly isolated area.

In case a communication is possible, the search-and-rescue operation can be directed in a much more efficient way because at this point the isolated people get in touch with the outer world and the rescue team gets to know details about their situation at an earliest possible point of time.

2.5 Central systems

2.5.1 Purpose

The purpose of Central Systems is to

1. configure the active underground network components
2. collect real time status information from the underground network components
3. store tracking records of the underground people and assets
4. enable network based voice and data communication to underground devices
5. display all information in location based context in a related mine visualization

Thereby, these IT systems are essential for regular operation during mine production in normal network mode as well as they act as important information source for rescue teams and decision making in the event of an emergency [98][87][101].

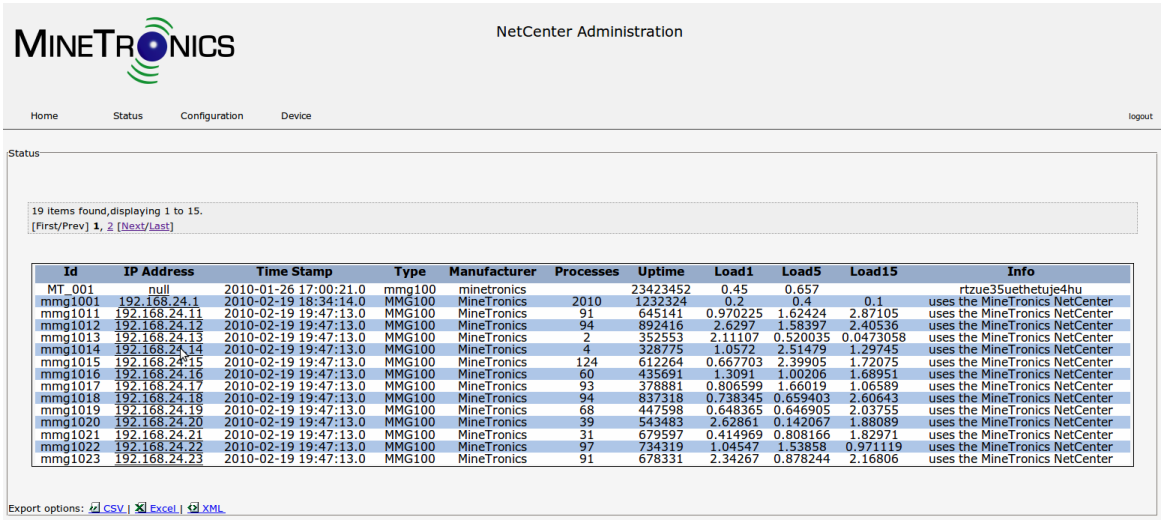
2.5.2 Network Configurations

The underground components working in a mine are often difficult to reach and getting to the devices often requires an entire shift. Therefore, all device configurations and upload of updated firmware has to be performed remotely without disturbing the ongoing underground operations, or impacting the safety of people. Therefore, a single central system, the "*NetCenter*" is used for the following standard functions carried out remotely [87] [101] [98]:

- configure underground devices
- store backup copies of their recent configurations
- instantaneous and time scheduled upload of firmware
- Provide real time status information about the underground device status and functional details

In addition, the NetCenter hosts or proxies all information relevant for the new Safety Support functions and their network related configuration (chapter 2.3.1 and figure 6) like:

- Static tunnel map
- Static map of safety equipment and conditions
- Static network layout map (hardware topology as built)



Id	IP Address	Time Stamp	Type	Manufacturer	Processes	Uptime	Load1	Load5	Load15	Info
MT_001	null	2010-01-26 17:00:21.0	mmg100	minetronics		23423452	0.45	0.657		rtzue35uethetuje4hu
mmg1001	192.168.24.1	2010-02-19 18:34:14.0	MMG100	MineTronics	2010	1232324	0.2	0.4	0.1	uses the MineTronics NetCenter
mmg1011	192.168.24.11	2010-02-19 19:47:13.0	MMG100	MineTronics	91	645141	0.970225	1.62424	2.87105	uses the MineTronics NetCenter
mmg1012	192.168.24.12	2010-02-19 19:47:13.0	MMG100	MineTronics	94	892416	2.6297	1.58397	2.40536	uses the MineTronics NetCenter
mmg1013	192.168.24.13	2010-02-19 19:47:13.0	MMG100	MineTronics	2	352553	2.11107	0.520035	0.0473058	uses the MineTronics NetCenter
mmg1014	192.168.24.14	2010-02-19 19:47:13.0	MMG100	MineTronics	4	328775	1.0572	2.51479	1.29745	uses the MineTronics NetCenter
mmg1015	192.168.24.15	2010-02-19 19:47:13.0	MMG100	MineTronics	124	612264	0.667703	2.39905	1.72075	uses the MineTronics NetCenter
mmg1016	192.168.24.16	2010-02-19 19:47:13.0	MMG100	MineTronics	60	435691	1.3091	1.00206	1.68951	uses the MineTronics NetCenter
mmg1017	192.168.24.17	2010-02-19 19:47:13.0	MMG100	MineTronics	93	378881	0.806599	1.66019	1.06589	uses the MineTronics NetCenter
mmg1018	192.168.24.18	2010-02-19 19:47:13.0	MMG100	MineTronics	94	837318	0.738345	0.659403	2.60643	uses the MineTronics NetCenter
mmg1019	192.168.24.19	2010-02-19 19:47:13.0	MMG100	MineTronics	68	447598	0.648365	0.646905	2.03755	uses the MineTronics NetCenter
mmg1020	192.168.24.20	2010-02-19 19:47:13.0	MMG100	MineTronics	39	543483	2.62861	0.142067	1.88089	uses the MineTronics NetCenter
mmg1021	192.168.24.21	2010-02-19 19:47:13.0	MMG100	MineTronics	31	679597	0.414969	0.808166	1.82971	uses the MineTronics NetCenter
mmg1022	192.168.24.22	2010-02-19 19:47:13.0	MMG100	MineTronics	97	734319	1.04547	1.53858	0.971119	uses the MineTronics NetCenter
mmg1023	192.168.24.23	2010-02-19 19:47:13.0	MMG100	MineTronics	91	678331	2.34267	0.878244	2.16806	uses the MineTronics NetCenter

Picture 4: NetCenter device status overview page

2.5.3 Real Time Status Information

The *NetCenter* also handles the real time status information coming from the underground devices [87][101]. This is information about:

- Power status (Device switched on, operating on mains or UPS battery power)
- WLAN status for each channel (ID of connected devices, link quality)
- LAN port status (e.g. connected, data exchange, packet statistics)
- Status information from auxiliary equipment connected to the network node like the power status of the UPS etc.

In addition, the link status information from all hardwired network links is compiled into a topology overview so the entire network topology can be visualized [101][87]. A history may be available to replay changes over time.

2.5.4 Tracking Server

A separate software, the *TrackCenter* is used for storing the tracking information for people and assets received from the underground devices. All data is stored including time stamps in chronological order to allow reproduction of movements over time e.g. after an emergency.

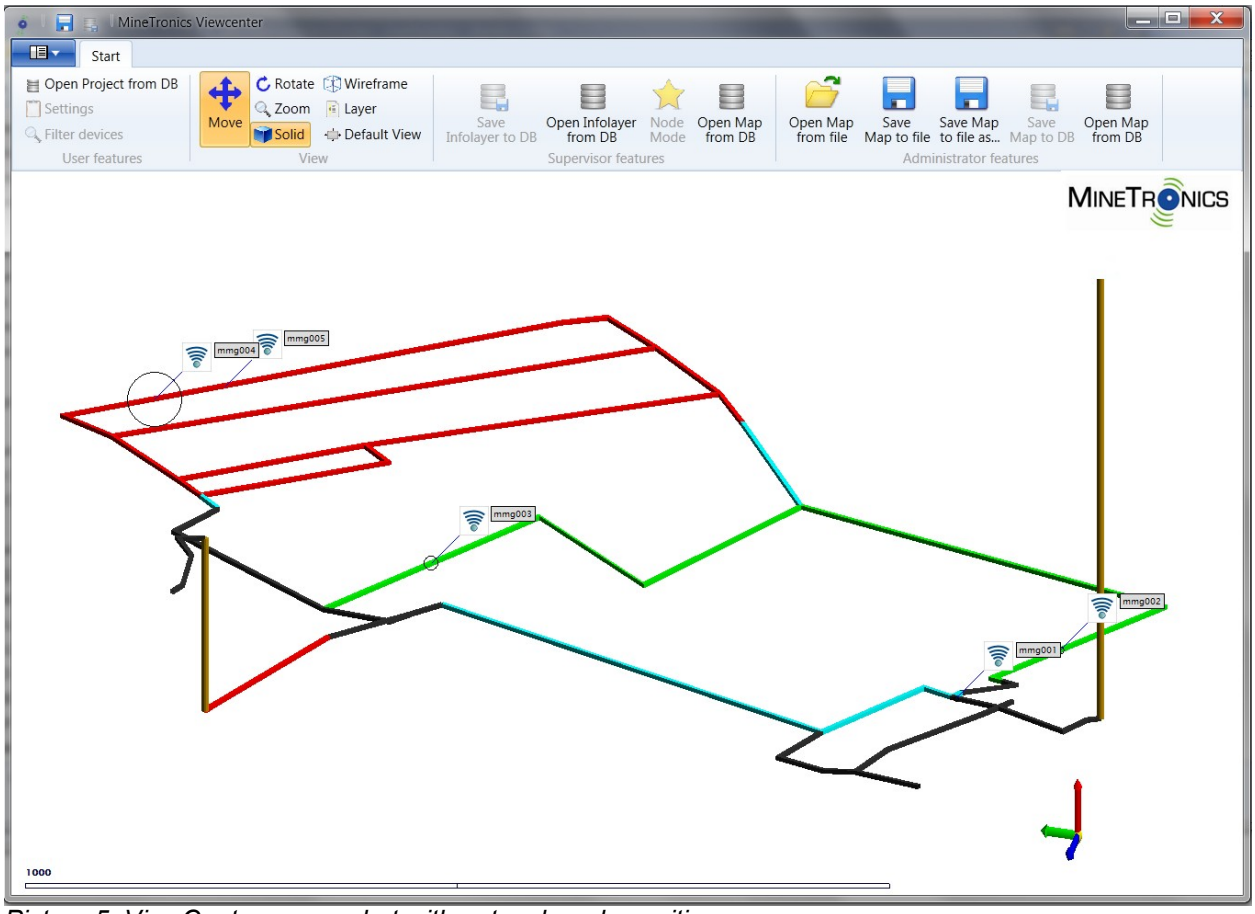
2.5.5 VoIP

The *VoIPCenter* is the central server software to organize VoIP audio channels. Consists of a standard SIP server and a web based user interface to conveniently group participants and to

switch loudspeaker lines and telephones.

2.5.6 Location based visualization

The basis for a location based visualization of the underground operations is an electronic mine map, preferably originating from CAD shown on the screen using a 3D visualization engine [54]. The information from all central servers in the system is communicated to the 3D visualization server ("*ViewCenter*") in order to be displayed on screen in different layers.



Picture 5: ViewCenter screenshot with network node positions

2.5.7 Distributed Architecture

Taking into account the high demands on the resilience of the network, the demands on the resilience and reliability of the Central Systems have to be at least similar. This is the reason for a preferred use small software systems with well defined purpose and well defined, clean interfaces among each other and for the use of clustered server system hardware to assure hardware redundancy.

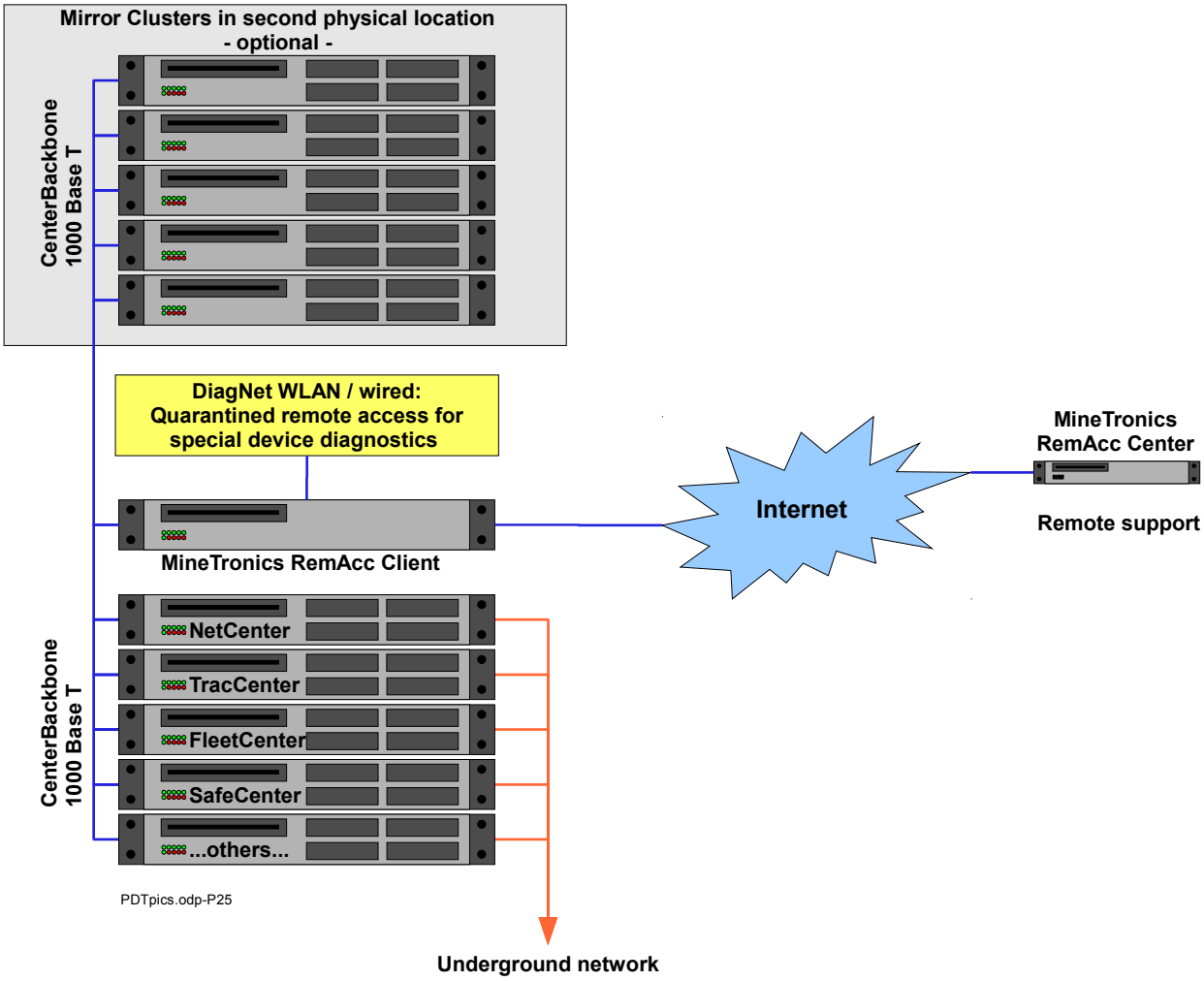


Figure 11: Redundant setup of servers with remote access [98]

2.5.8 Connectivity to external systems

As a mine is a highly dynamic "*moving*" raw material factory, the central systems ideally need to be setup up in a way that the permanently changing infrastructure of the mine is updated automatically. For this purpose an access to the Geospatial Database of the mine is needed.

This database then is the directly connected to the 3D mine visualization software which either imports the geospatial data in fixed time intervals (e.g. daily or weekly) or it is directly connected to this database.

According to [54] this has earlier been realized with the 3D visualization software used, however it often requires a significant customer individual development effort. Today however using modern information exchange routines like the Geographic Markup Language (GML) [85]

have the potential to simplify implementations if supported by all systems involved.

Further external interfaces are needed as outlined in earlier chapters for all safety relevant sensor information [115][98][20]. In contrast to current implementations, these interfaces also need to be available underground without requiring active communication to above ground central systems.

3 IMPLEMENTATION OF UNDERGROUND HARDWARE

This chapter explains the general implementation of the Ethernet based Mine Communication System explained in chapter 2 and focuses on the implementation details of the networking hardware in use underground.

After explanations about the specification and operational prerequisites (3.1) the chapter explains the implementation of the network infrastructure systems for underground use (3.2) and mobile field devices for application use (3.3).

3.1 Introduction and Specifications

3.1.1 Introduction

The following chapters describe the architecture and implementation of the new, network based underground communication system capable to fulfill the functionality outlined in the previous chapter. This system is used for the following purposes:

- Under regular operation it provides the regular wired and wireless network communications for process optimization, automation, voice communication etc.[112].
- In case of an emergency, the network and especially the active network nodes underground provide important support functions to handle the emergency case and to provide rescue teams above ground with all information available to support a quick, efficient and safe rescue operation [125].

This conforms a complex system consisting of distributed hardware and software components: The active network hardware underground is equipped with built in application functionality and safety support functions in order to enable the system to survive and provide all safety support functions of the network even if connections to above ground systems are lost.

The implementation has to take into account four different use cases for system operation which have to be realized in a way so that all components available in a certain use case have all

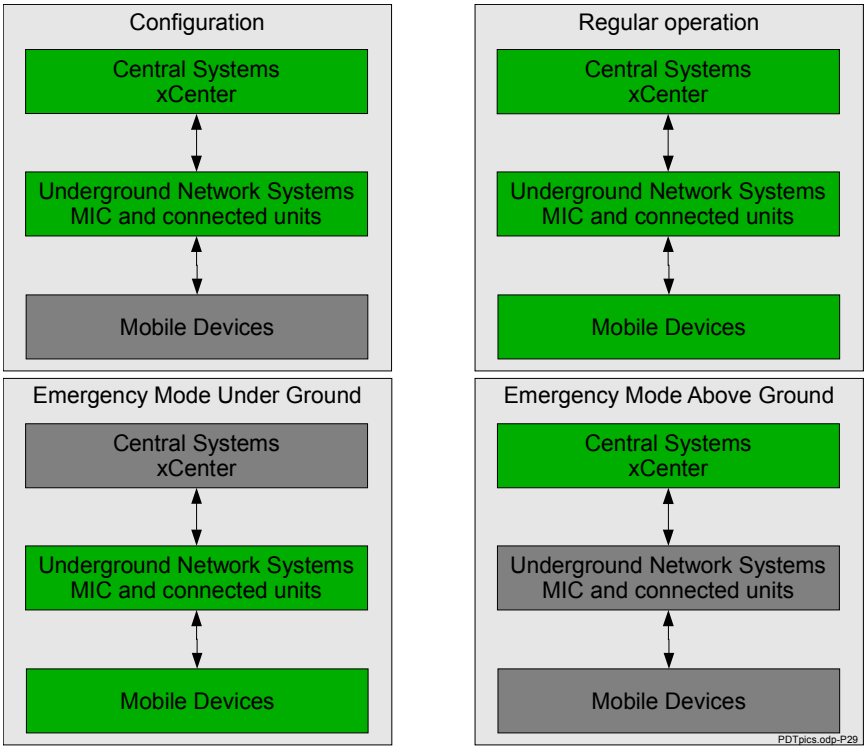


Figure 12: Use Cases of the system and active components (green)

information available to perform their tasks (figure 12). These use cases are:

1. **Configuration** of the system and it's components at initial startup of the entire system and at startup of singular system components (new or restarted) in regular operation or when configurations change in regular operation
2. **Regular operation** with all system components functional
3. **Emergency Mode operation** with only the **underground** components available for all users underground in an Emergency Case
4. **Emergency Mode operation** with only the **above ground** servers available for the users above ground in an Emergency Case

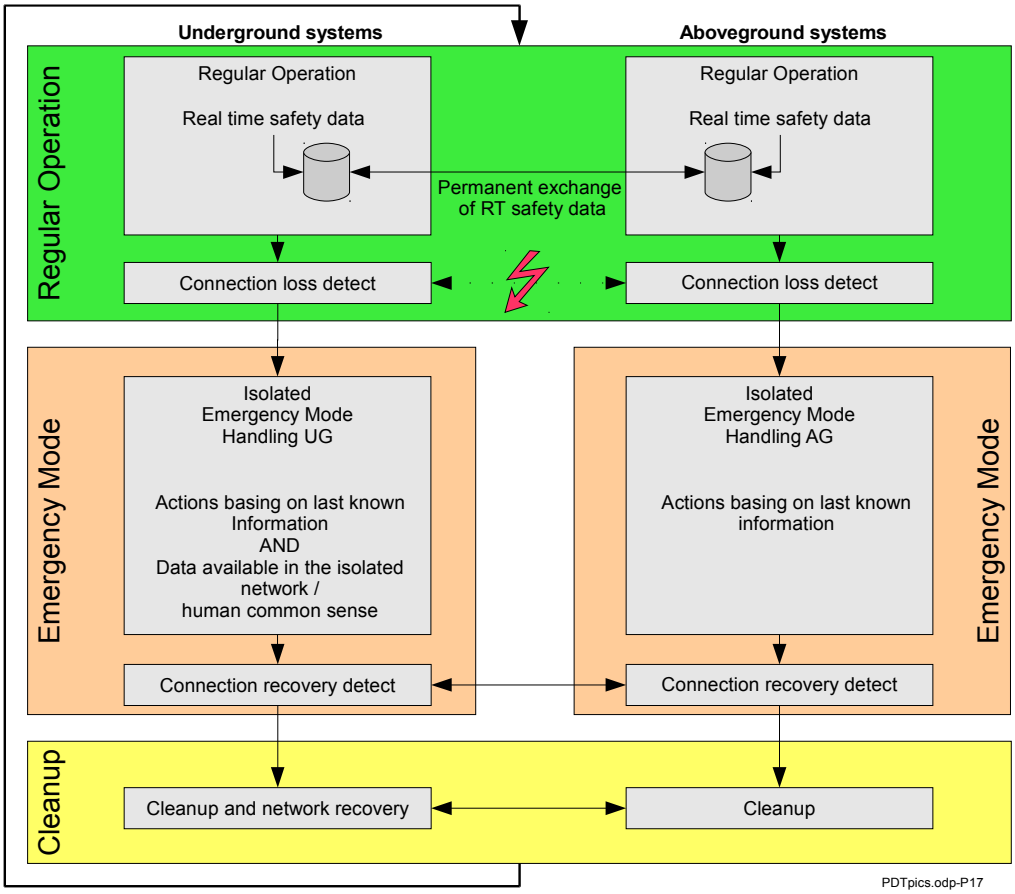


Figure 13: Split Processing in Emergency Mode

These different operation conditions are connected in the sequence shown in figure 13. after connection loss all processing is split off between underground and above ground systems while they have to resume regular operation after the connection is re-established. The operating conditions during the time of split operation are more or less incalculable due to the dynamic

nature of any emergency situation.

These use cases set high demands on the hardware especially in terms of reliability and processing power of the underground systems and on the functional implementation of the entire system especially in terms of keeping all data synchronized between underground and above ground systems in regular operation mode so the pictures on the situation are far most identical on the central systems above ground and on the network nodes underground when a switchover to Emergency Mode occurs.

Due to the fact that Ethernet based networking especially in underground coal mining due to explosion proof regulations is lacking of many devices, this project beside the functional implementation has to solve both the availability problem for the infrastructure but also provide field devices to make this new infrastructure usable. Therefore it gives also the chance to develop all required devices in a way that they have the potential to fulfill the demands on safety support functions outlined in section 2 of this thesis.

For this implementation project a number of external dependencies and preconditions have to be given in order to be able to demonstrate the full functionality. These are not technological but mainly operational issues which are not easy to meet in an ongoing mining operation environment:

1. The availability of a mining site for a large scale implementation which in the end also allows testing and certification of the Safety Support functions.
2. Availability of external interfaces to third party environmental monitoring equipment as used by the mine.
3. Certification of the hardware to relevant Ex protection standards (EN60079) [29][41].

3.1.2 Specifications and project limitations

Specifications are subject to dedicated distributed documents each covering an individual product involving the safety support features described in this document [98][87]. For not extending this document beyond the intended size, the specification matrices are not explained here in detail. In order to reach a functional system at an earliest possible stage, all specifications for the project are grouped in three categories [119][116][98]:

1. The specified item is required for the basic system to work. It is thereby required to implement this item before a first basic application is ready to start

2. The specified item is an important option but not required for the basic system to start
3. The specified item is a future option or a "*nice to have*" which is implemented only if it does not impose significant additional implementation work or within a new, separate project

The project is limited to provide the basic safety support applications and infrastructure functions. It presumes that in the application mine a fiber optic Ethernet network infrastructure is available, which is extended to above ground central systems via at least one shaft. Devices and systems potentially supplying the new network based safety support system with external information like mine environmental monitoring or automation systems are not part of this project.

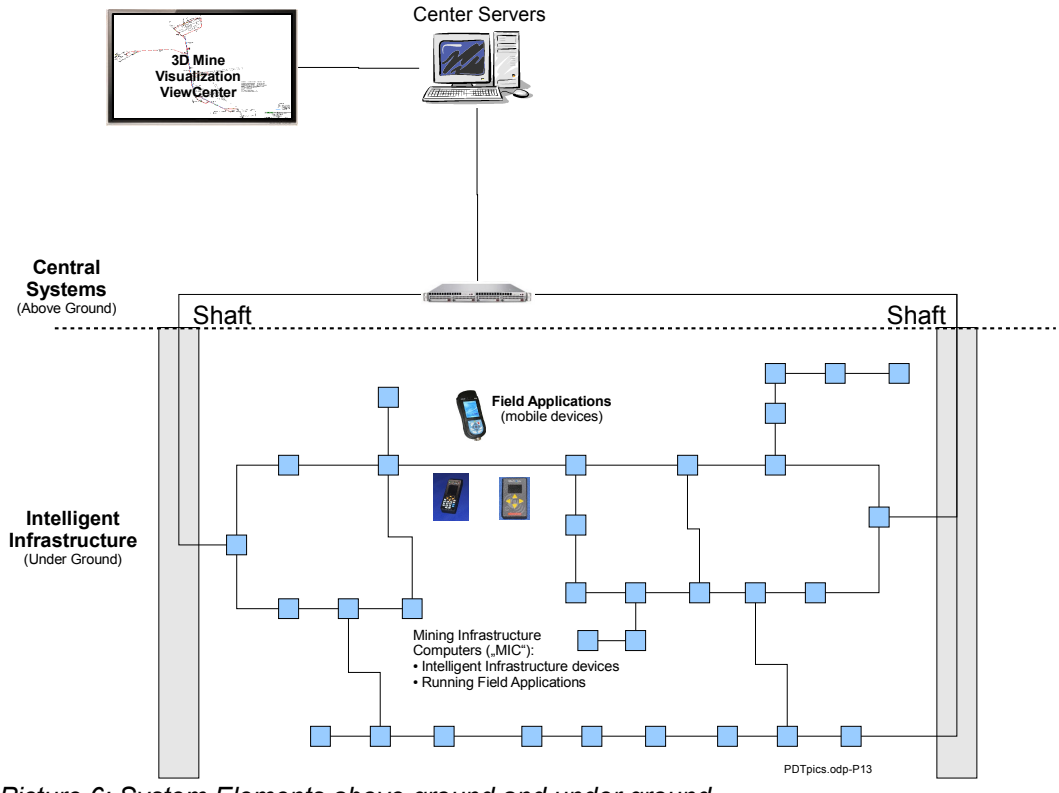
3.2 Network Infrastructure Hardware and Equipment

3.2.1 Overview

The system hardware components consist of the following groups of devices[119]:

1. Intelligent Infrastructure (this chapter)
2. Field Applications (chapter 3.3)
3. Central systems (chapter 4.1)

The "*Intelligent Infrastructure*" consists of network components capable of turning data originating from the network (status of nodes, status of links) potentially in combination with other data available locally (environmental, ventilation or gas sensor values) into information to support underground safety. In an emergency case, such information may be used to give advise to people how to behave in emergency (e.g. to prevent them from walking into dangerous zones etc) [116][119].



Picture 6: System Elements above ground and under ground

"*Field Applications*" cover mobile client devices worn by people or mounted on vehicles as well as stationary network clients used for communication with people. This could e.g. be VoIP devices or personal devices for tracking people in the underground infrastructure) as well

as network devices as e.g. lamps or TFT displays showing dynamic emergency information and / or escape routes [119].

"*Central Systems*" are used above ground to store and visualize information from the underground network as well they store all information related to underground safety in order to:

- Download static safety information (e.g. location of safety equipment) to the Field Applications under regular network operation.
- Help rescue services to evaluate the situation under ground in case of emergencies [87]

Both *Central Systems* and *Field Applications* are important in case of an emergency. In this situation the communication to under ground may be cut, so if people under ground behave as the Field Applications propose, the central systems due to their situation knowledge and knowledge of the algorithms of the field systems eventually may help to predict the behavior of the people under ground in order to dispatch the rescue teams efficiently to those places where the underground people may be located.

These three parts are described in deeper detail in the following chapters:

3.2.2 Intelligent Infrastructure

Traditionally, networking infrastructure is regarded passive in terms of application functionality: It is simply used as a carrier for any kind of information in the way the infrastructure is configured for.

In underground mining, the network infrastructure always has to follow the tunnel line of the underground roadways. Active network components like switches mostly are installed close to junctions where adjacent tunnels meet as this is the most efficient way to interconnect cables.

This way, the network infrastructure perfectly mirrors the layout of the underground mining structure: Tunnels with a working network link can be regarded as OK while e.g. in case of an accident a suddenly missing network link can be an indication for a collapsed tunnel structure, an explosion etc.. This fact is one basis of the patent application related to this thesis [115].

„*Intelligent Infrastructure*" means that such information from the infrastructure is used for operational and safety purposes and that the active infrastructure components are able to provide and process such information for safety purposes [113].

All active components in the infrastructure today contain embedded computers which

mostly are not use for purposes other than forwarding data packets. This computing capacity in an already certified unit is used for the additional safety purposes making the infrastructure "intelligent" from an application or safety point of view.

Thereby the network infrastructure and especially it's active components are used for a number of additional functions beyond the pure handling of network data packets:

1. Detect places of potential accidents [120][118][115].
2. Inform people under ground about the next available emergency exit, safety shelter etc: When the network to an exit still is alive the probability is high that the way for people to this exit is open, too [120][115].
3. Locally compute important environmental information to inform the people in vicinity even if the connection to the above ground systems is lost: Gas content of air (CH4, CO etc), Airspeed and -direction, etc. [115].
4. Automatically switch into a safety mode when connections to above ground are lost in order to provide functional network islands to keep people in these islands to communicate with each other and to let them localize each other [115].
5. Locally inform people by messages to their mobile devices, by LED flashes integrated into the infrastructure devices („*Lighthouse function*") and by an optionally built in display [115].
6. Automatically try to find new network routes to above ground when the default connections are lost. This is performed by setting up meshed network structures either wired or wireless [115].
7. Tracking of men and material using the wireless network as a detection criteria [115].
8. Tracking of material using attached RFID readers
9. Acting as base stations for accurate positioning and sensor network applications

In respect of all additional functionality the networking devices are set up as standard networking units basing on the unmodified available industrial standards.

3.2.3 Mine Infrastructure Computer („MIC“) System

The intelligent Infrastructure is implemented using a central networking component named „*Mining Infrastructure Computer*“ or „*MIC*“ [120].

This unit provides all networking functionality and in addition all distributed application level computing power required for distributed functionality and related mine safety support. The majority of all safety support functions described in this document are running on the Mine Infrastructure Computers [116], which was entirely developed and certified within the project [92][58].

Due to the requirements for the Ex approval [29] the entire system is structured into a System and Functional Modules. In this setup, the System defines the setup with external enclosure and the connection of external electric devices and the Functional Module contains the electronics providing the functionality of the system [92]. One System in the sense of the ATEX certification may contain 1-n Functional Modules.

The MIC System is set up as a stainless steel outer enclosure (Picture 8) mounted underground in a mine (Pictures 7).

Picture 7: MIC system in underground installation

Picture 8: MIC System in delivery shape

The system enclosure contains the electronic modules and auxiliary components for power supply and a patch field for fiber optic network distribution (Picture 9). In this picture, the system contains three Functional Modules: The central MIC (left), an RFID reader (mid) and an

additional switch (right). This system enclosure provides space for four Functional Modules.

Picture 9: MIC System internal setup

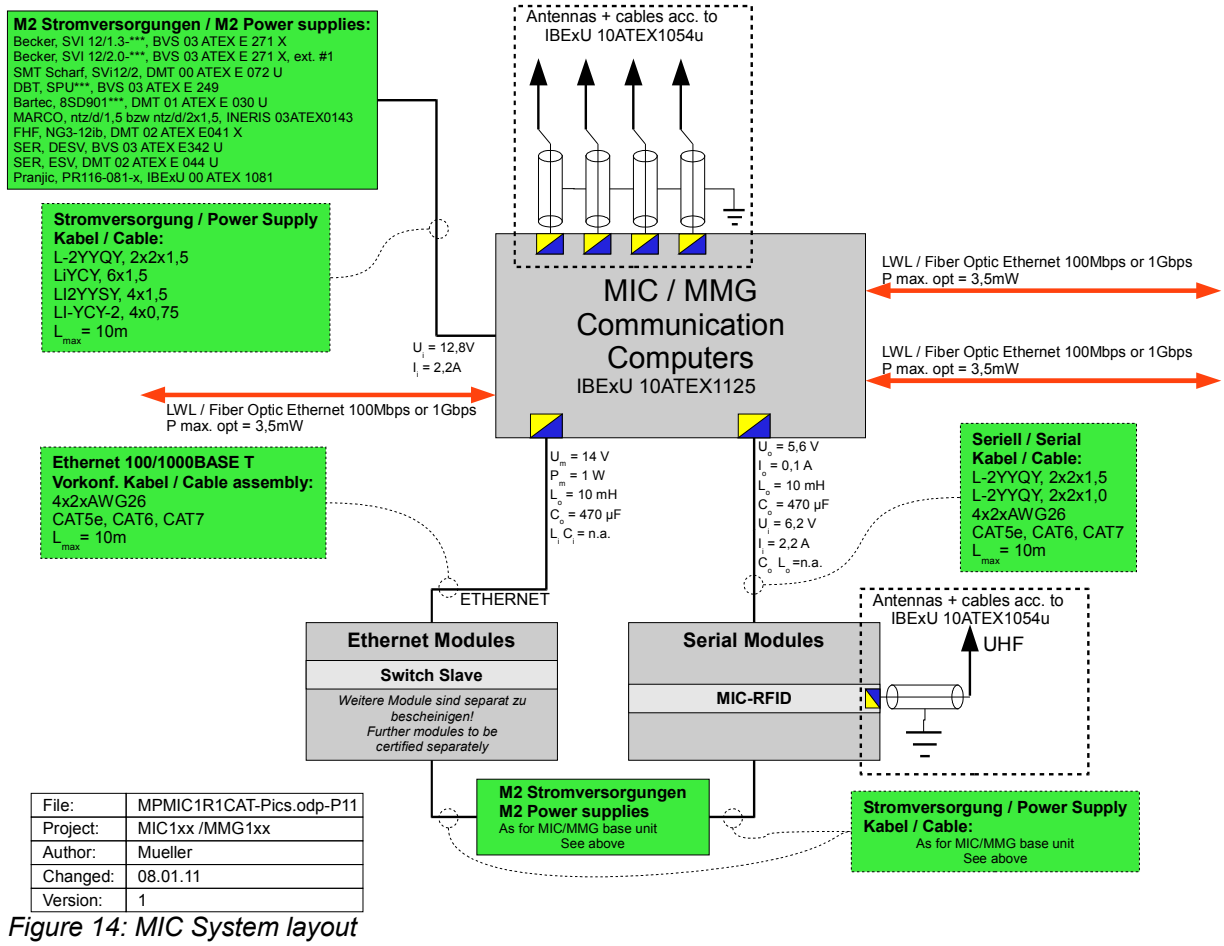


Figure 14: MIC System layout

For use in potentially hazardous environments subject to certification in accordance to EN 60079 [41][29][28], all system components have to be uniquely identified covering power supplies, cables and all components relevant to intrinsic safety as well as the related electrical parameters of the interfaces. The resulting system overview chart is shown in figure 14. with the grey modules representing functional modules of the MIC system as described below in the following chapters.

3.2.3.1 MIC CPU Module

A MIC CPU Module is the central processing unit of the underground network to provide safety support functions[116][92]. It consists of:

- A network processor board incl. two independent WLAN interfaces
- One fiber optic Ethernet switch module
- An individual, custom made base board containing safety circuits to assure intrinsic safety in terms of prevention from CH4 explosions and containing a microcontroller to supervise the unit and to handle external peripherals as well as the power up process.

After assembly, all components are encapsulated in a silicone compound.

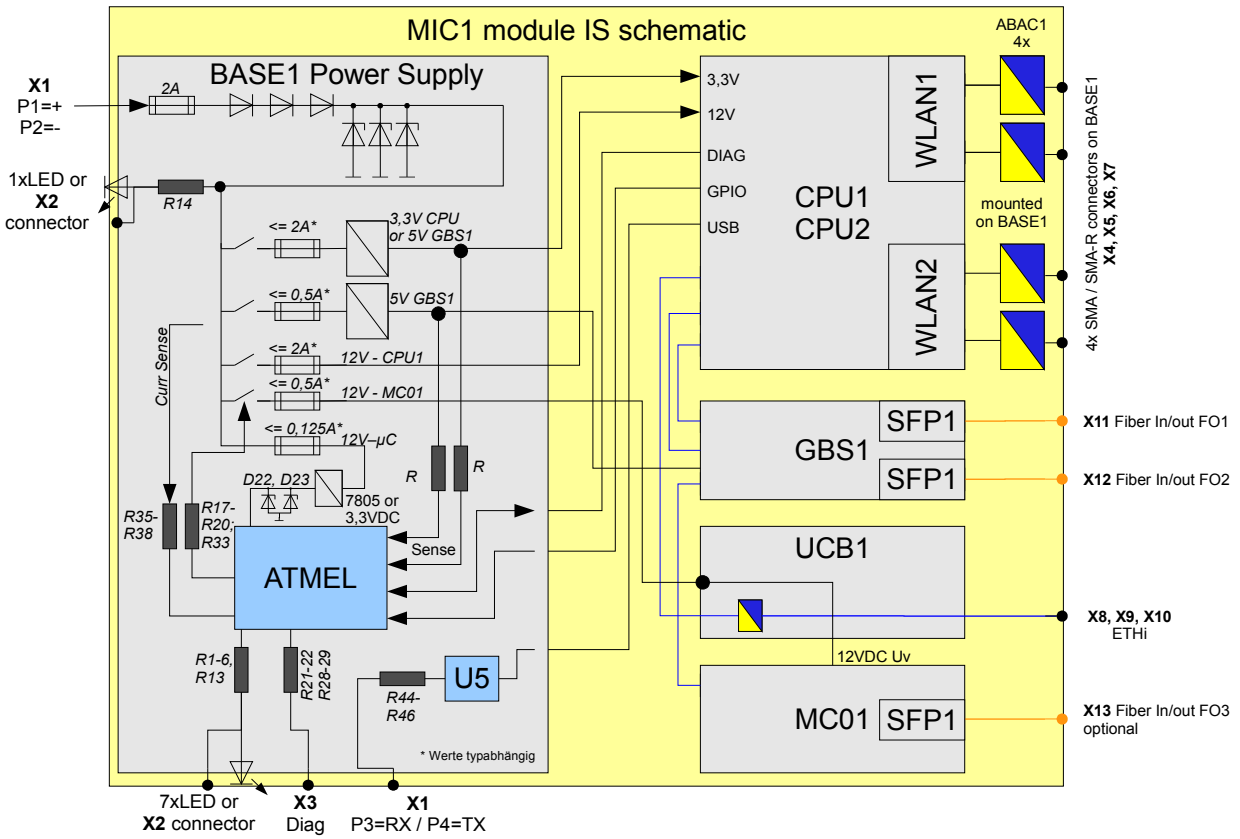


Figure 15: MIC module block scheme ("IS scheme")

3.2.3.2 Power Supply Board

The BASE1 internal component provides internal power switching logics and takes care of the intrinsic safety of all other external electrical connections. This is mainly assured by limiting voltage and current on the external electrical lines by diodes, Zener diodes and resistors (figure 15). For AC coupled external components like antennas capacitive barriers are used to achieve a sufficient DC potential separation [26] [27]. Other interfaces like serial ports have to be decoupled by opto couplers (U5). Dimensioning of all these components is subject to certification basing on relevant checklists and calculation tables.

As certification needs to specify components, PCB layout and production quality assurance, the BASE1 component is a PCB custom developed for the MIC. The main function is to convert the incoming voltage of $12VDC_i$ (*i* for "*intrinsically safe*") to the voltages used by the other components in the device.

The incoming voltage first runs through three linear diodes for reverse voltage protection and to prevent from currents to flow back out of the device [27]. Three elements are used in order to provide a two failure safety as required for "*M1*" certified devices acc. to EN 60079-11 [26]. "*M1*" devices are allowed to remain powered when the main electricity is switched off due to hazardous gases (Methane) detected in the area [26].

The Zener diodes are used in acc. to EN 60079-11 [27] as a protection against excessive voltages and inductance flowing back from the device.

Via an additional small fuse and a linear voltage converter the voltage then is permanently powering the ATMEGA microcontroller (AVR32). The additional fuse is needed to meet power limits in accordance to EN 60079-11.

The microcontroller controls the MOSFET switches for four device internal consumer power lines, which also are equipped with separate fuses. This is to assure that during startup the power up of the connected devices can be controlled sequentially in order to reduce the startup current spike so the external intrinsically safe power supply does not activate it's safety circuits when the device starts up.

3.2.3.3 CPU board

The CPU board is an off-the-shelf assembled PCB [161] which mainly combines two independent copper Ethernet ports, three Mini-PCI slots for WLAN cards and an Atheros CPU.

The selection of this component was performed basing on a Multi Criteria Analysis covering seven alternative products and the following criteria in the ranking as mentioned [109]:

1. Development and System integration Effort / Time needed
2. Low development and System Integration Risk
3. Hardware Component Purchase Cost
4. Ex certification Easiness
5. Functional Completeness
6. Production Simplicity
7. Long Term Component Availability

This ranking was chosen due to the fact that at the beginning of the development a basic product had to be available very quickly. A similar evaluation was performed for the successor model designed in 2012 where the following ranking was applied:

1. Functional Completeness
2. Low development and System Integration Risk
3. Production Simplicity
4. Hardware Component Purchase Cost
5. Ex certification Easiness
6. Long Term Component Availability
7. Development and System integration Effort / Time needed

3.2.3.4 Wireless LAN

To provide the wireless LAN functionality on two different channels or frequency bands, two standard Mini-PCI WLAN cards are mounted into the CPU module. For best possible RF propagation in mining environments, WLAN cards with antenna diversity output are chosen [36] [86].

3.2.3.5 Fiber Optic Switch

As fiber optic switch another assembled PCB module for industrial use was chosen [108]

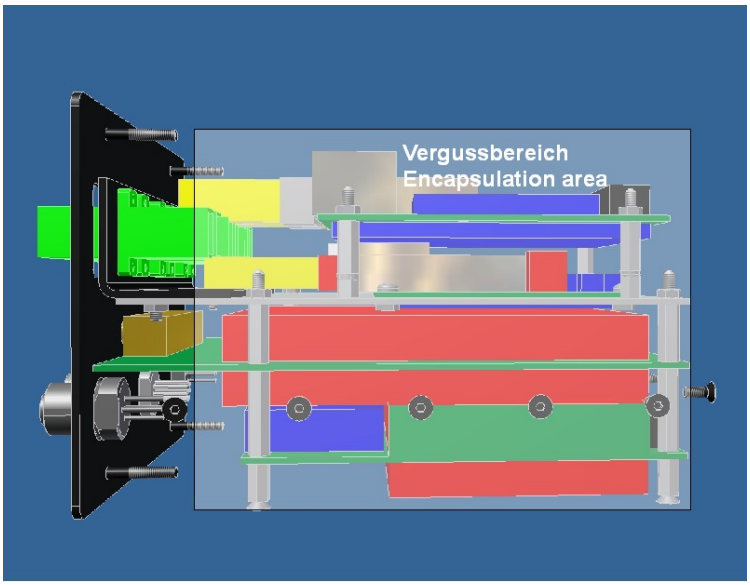
after a tender to manufacturers for a custom made board was unsuccessful [102]. The selected component provides a fully managed Gigabit Switch with three copper and two fiber optic ports which can be flexibly used by different SFP ("*Small Form-Factor Pluggable*") transceiver modules [146]. This enables the use of both 100Mbps and 1 Gbps Fiber Optic Ethernet to be used during production of the MIC modules.

The managed switch core used is a Marvell chip as commonly used in many industrial products.

In order to provide three Fiber Optic outputs, an additional media converter is used to convert one of the copper ports into an additional fiber transceiver.

3.2.3.6 Mechanical construction and manufacturing

The device is built up as an electronics stack with the PCBs connected to each other using standard distance bolts. After this stack is tested on functionality it is assembled into a steel enclosure where it finally is encapsulated by a soft silicone compound for protection against moisture, to enhance temperature behavior and to exclude potentially dangerous gases in ATEX environments (picture 10) [92].



Picture 10: MIC internal construction with encapsulated area

Using an intrinsically safe encapsulation in accordance to EN 60079-11 is the most flexible form of meeting the standards for intrinsic safety in terms of design and certification procedure. However, the disadvantage is that the device is fully potted by encapsulation compound which has to be filled into the enclosure in liquid form surrounding all electronics.

Especially the encapsulation of the fiber optic transceivers is a challenge which is not easy to meet in the manufacturing process. The challenge with the fiber optic transceivers is to prevent the encapsulation compound from moving into the transceiver plug thereby potentially attenuating the optical signal. The Silicone encapsulation compound used has a standard viscosity of [167] which may creep into the transceivers by capillary effects. Therefore, an additive ("*thixothropic Additive*" [168]) is used to increase viscosity which in turn safely prevents the compound from moving into such structures.

An additional advantage of encapsulation of the devices is the improved thermal behavior of the electronics due to the monolithic block of silicone compound of significantly better heat dissipation than free air inside an IP54 enclosure.

3.2.3.7 Network integration of the MIC network node

As explained with the hardware setup, a MIC system consists of the network node itself with CPU board and one managed switch module. In addition, separate "Slave Switch" devices can be optionally connected to extend the number of physical network ports available (fig. 16). Each Slave Switch devices in turn consists of up to three managed fiber switch PCB-A modules. All Slave Switch devices together with one MIC CPU module conform one MIC System in one particular location in the mine.

For this device, the universal base board and the existing switch modules were combined in a separate enclosure which is some centimeters bigger than the original MIC. This switch is also integrated in the safety functions by the CPU of the MIC it is attached to. Also the ports on this switch can be supervised from on the LCD display of the main CPU.

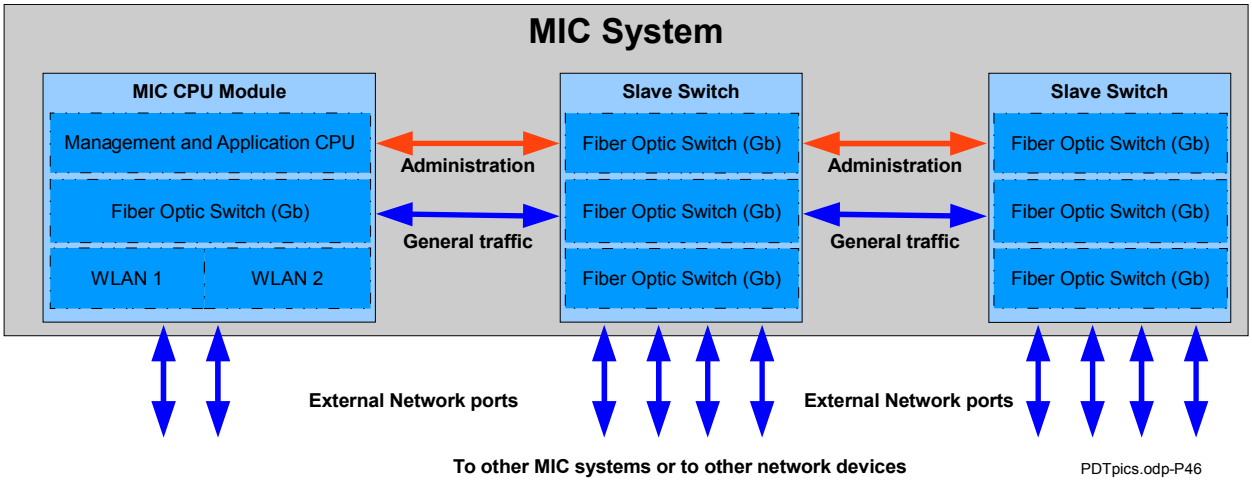


Figure 16: MIC System Setup

For user convenience, the administration of all devices in one system (MIC CPU, WLAN, Slave Switches and potential other peripherals) has to be carried out via one single Web User Interface residing in the MIC CPU [91]. This requires a separate logic administration network among the devices in a single MIC system, which is implemented as a reserved local private subnet, which is used exclusively among the network based modules inside each MIC system.

This subnet is blocked to the outer world by running inside a reserved virtual LAN (VLAN) which is blocked on all external ports making this subnet physically inaccessible outside the MIC system. This VLAN is only available on the internal administration ports of each physical switch module used.

To access the different modules in one system, a unique identification method is required. This is performed by deriving the IP addresses in the Administration network from the serial numbers or MAC addresses of the components used. Internal traffic for administration, configuration and also for the neighborhood determination of the Safety Support functions (chapter 4.3) uses this network.

3.2.4 Independent power supply

All intelligent infrastructure will need power backup units for at least 4 hrs independence time in order to be capable of running safety related functionality.

For this purpose, an intrinsically safe battery backup power supply is needed. As a suitable power supply was not be possible to be purchased from a third party supplier (as planned in the beginning of the project) it was decided to develop a related unit as part of the underground network system. The independent power supply development is currently ongoing.

Traditionally, intrinsically safe battery power supplies for use in underground mining are built up as single units for direct primary supply from 110-240VAC and an intrinsically safe secondary output on 5 or 12 VDC.

Disadvantages of this design are the fact that they are extremely heavy (more than 50kg) and an exchange of the battery cells is not possible in the underground environment, meaning that the heavy devices has to be taken to above ground and sent back to the manufacturer for cell exchange.

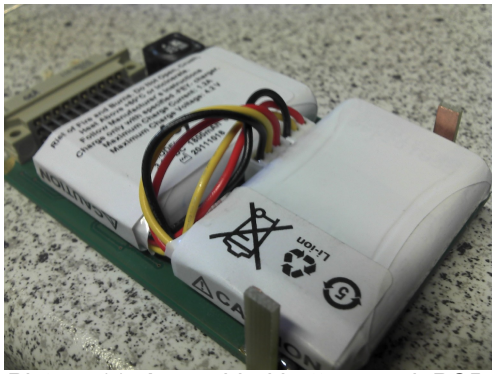
Therefore, the new design was created as a completely intrinsically safe unit which is powered by separate intrinsically safe power supplies so the UPS unit is supplied with

intrinsically safe 12 VDC inputs. Two inputs are used whereof one is for the online supply of the connected devices and the other to supply charging power for the battery packs.

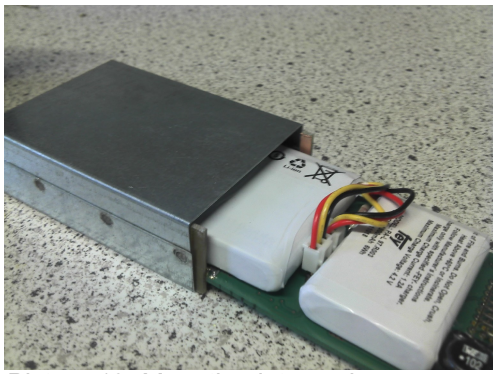
As one single intrinsically safe unit is limited to about 25W in order to keep to the definitions of intrinsic safety in acc. to EN 60079-x, the power handling inside the device is a challenging design task: It has to be assured that the consumer path (which reaches about 20W) never can be connected with the separate charging path.

3.2.4.1 Intrinsically safe Battery Packs

Basis of this design is an intrinsically safe battery pack developed basing on a a specific LiIo cell technology ("*PSS*" from Panasonic) [134] [135], which keeps the risk of runaway situations comparatively low. These cells were officially tested by the notified body resulting in cell shortcuts causing no higher temperatures than 115-120°C at the maximum ambient temperature of 40°C [59]. From these cells, a battery pack was designed consisting of two cells in row with a total accumulated power of about 12Wh, a LiIO battery pack controller (ATMEGA406) [3] and two separate and independent cell balancing safety circuits [159] as second level protection. From the functional point of view this provides three independent cell safety controllers especially to prevent from overcharging making the design resistant to two failures [89].



Picture 11: Assembled battery pack PCB



Picture 12: Mounting into casing

A hardware logic implemented by MOSFET-transistors assures that a single battery pack can either be charged or discharged. Thereby it is impossible that electrical power can dissipate between the charging and discharging circuits which in turn assures that the certification rule of up to 25W in a single intrinsically safe circuit can be met [89].

Precisely as the MIC, the battery pack also is manufactured inside a steel enclosure and encapsulated in silicone compound. In this case the silicone has another advantage of being

flexible allowing the cell's mechanical structure to change over time.

The battery pack as a micro controller controlled "*smart battery pack*" is equipped with an electronic I²C bus interface for communication with a main CPU. Via this interface all online data like charge status, voltage and current is available as well as historic data like number of charge cycles, Watt hours discharged and charged etc. [96].

3.2.4.2 UPS implementation

The UPS consists of 6 – 24 battery packs described in section 3.2.4.1. These battery packs are all connected to two separate internal power bus bars for charge power and drain power respectively.

Charge power is connected directly from the connected power supplies to the charge bus bar, while the discharge power is routed through a step-up type DC converter to bring the output voltage up to the required level of 12 VDC.

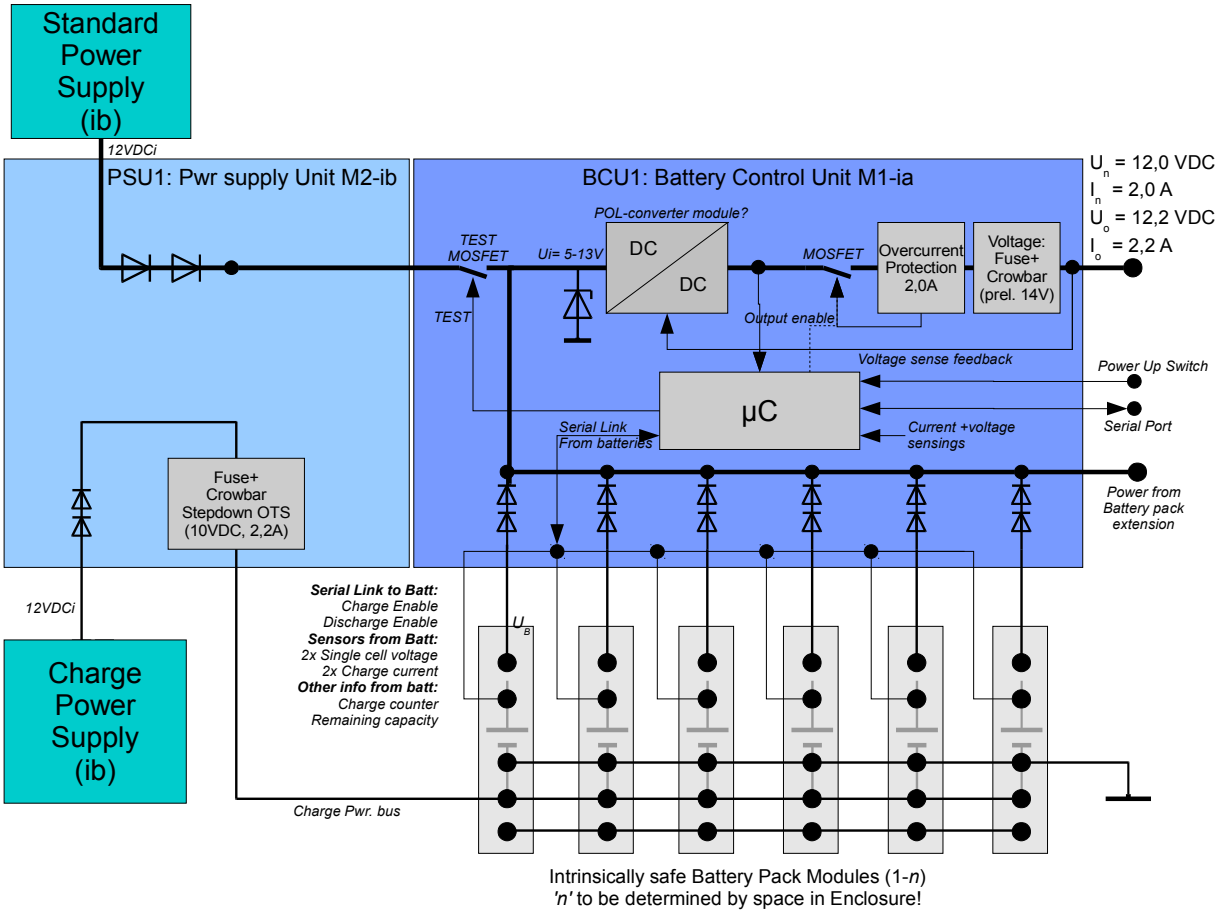


Figure 17: Block Schematic of intrinsically safe UPS

Charging and discharging of the battery packs is controlled by a central micro controller

of type ATMEL AVR32. Basing on the charge status of each individual battery pack, this controller switches certain battery packs into charge mode when external power available, while two other battery packs at the same time are in standby for being discharged.

When mains power is cut, the controller switches over to other battery packs for discharge as soon as the discharge level of the currently active battery packs is reached. By this procedure, all battery packs except of one are discharged. One battery pack always has to provide power to the micro controller in order to enable switching back to regular mode and to start charging when mains power returns.

An additional LCD display is connected to the main controller PCB as user interface beside the serial port which connects the UPS to a MIC type network node (see 3.2.3.1).

3.2.4.3 Battery Pack and UPS tests

Testing of the Battery Packs is an important phase especially for a product which is critical in function and critical in terms of Explosion safety, a matter which is even more critical by the use of LiIo cells. Therefore the product verification is performed in two stages: First all testing for design verification as part of the implementation and verification process and the second stage including all verification of the individual final products against the tests carries out during design in order to assure they are manufactured in accordance with the design document and verifications during the design phase.

The verification of the design included:

1. Testing all safety circuits for charging / discharging [89]
2. Testing all ATEX certification relevant safety circuits [89]
3. Verification of the thermal behavior [138] [53]
4. Running charge and discharge tests within design limits [89]
5. Exceeding the design limits during charging and discharging [89]
6. the produced units in a controlled way which gives an overview of the entire behavior of the [138]

In addition, the Certification body demanded a Thermal Equivalence test. This test was to assure that no overheating of the enclosure over 150°C surface temperature acc. to EN 60079-11 is possible, if in case of an internal error the maximum charging energy of 8,5W (10V/0,85A) is

converted into heat inside the battery pack. This test finished with an outside enclosure surface temperature of 62°C at an ambient temperature of 23°C [53].

In the prototyping stage of the UPS development, a number of tests were performed as a proof-of-concept in order to assure that the single parts of the design are working. These tests included the proof of concept of the entire power line and the efficiency of the step up converter. The latter is crucial for overall device performance as also the incoming voltage has to be routed through this converter even when the UPS is not supplying from batteries.

The entire operating range of the step up converter is defined from about 6,8 V as the lowest allowed voltage from a battery pack up to 11,5 V as voltage from the intrinsically safe mains power supplies after reduction by protection diodes [150].

The efficiency measured is shown in figure 18.

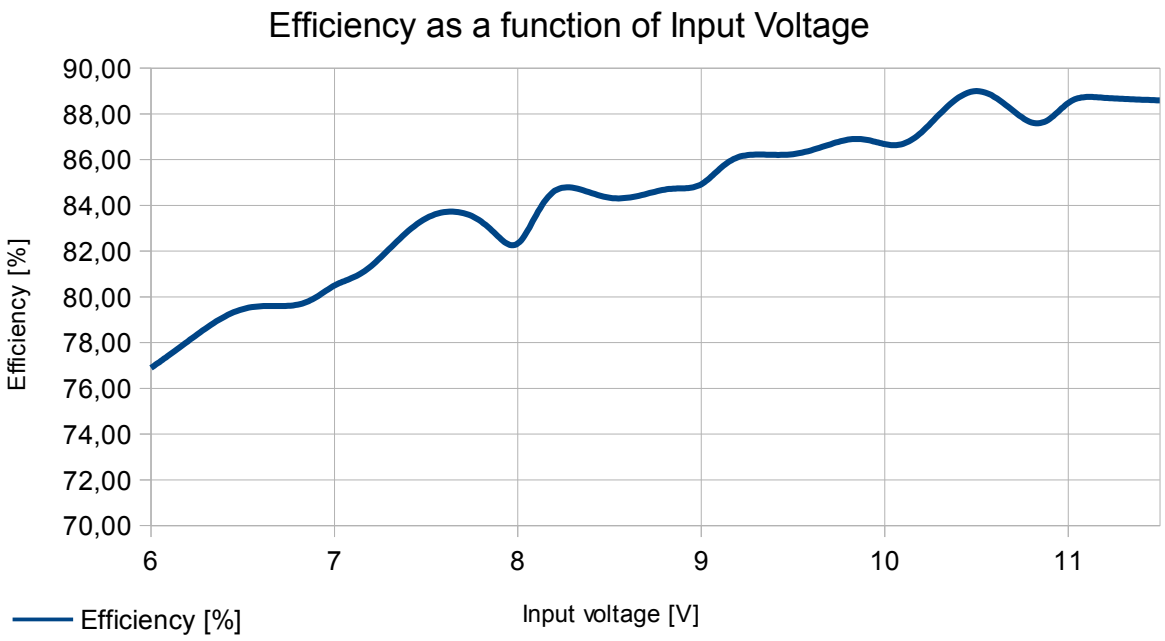


Figure 18: Step Up Converter Efficiency [150]

The Battery Packs are already in series production for use in an automation system. For production special test devices have been produced which automatically perform the final testing with controlled charge and discharge over two cycles while logging all relevant parameters on a PC. The UPS is still being to be finally tested and approved.

3.3 Field Application Systems

The field applications with relation to underground safety and safety support cover the following:

1. Personal Communication
2. Mobile Machine Communication
3. Man, Machine, Material and Asset tracking
4. Accurate positioning applications
5. Environmental data and sensor information
6. Network support for Search-and-Rescue teams

There is a large number of potential field applications, even such which not can be planned for today. Therefore, a related system design should allow for flexible extension to new functionality [119][117].

A number of field application devices can be used in a multifunctional way fulfilling more than one of the above mentioned functions.

3.3.1 Personal Communication

Personal communication covers all network enabled personal devices a miner could carry with him, as e.g.:

1. VoIP telephones (See separate specification document [117])
2. Mine Radios (basing on WLAN and UHF)
3. Pocket PC's [32]
4. Messengers (Pagers) [113]
5. WLAN or sensor network Tags for simple tracking

These devices can be personal devices (statically assigned to one specific person) or they are shared among the people and assigned dynamically when a person goes under ground. The system design allows both regimes to be applied simultaneously.

In case of a dynamic assignment, a personalization has to take place prior to the person entering the mine. The system concept takes this into account, however individual projects are

required for each implementation on a particular mine as this functionality is highly dependent on the individual IT systems used and the mine individual user identification system and processes used.

The personal devices may be bought off-the-shelf like the PDA shown in picture 13. The system design of the Safety Support functions does not require them to be MineTronics proprietary devices. However, if such devices are developed within MineTronics, they may provide additional safety support functions not available in off-the-shelf equipment.

An important MineTronics proprietary feature of such devices is that they have to be capable of interacting with the intelligent infrastructure to display safety messages etc. This could be a pure software feature to be implemented on any off-the-shelf device (like the PDA in picture 13).

Picture 13: Personal Digital Assistant (PDA) for underground use

Personal devices shall support the following safety support functions:

1. Being tracked by the "*Intelligent Infrastructure*" (see 3.2.3)
2. Acoustically warning the person when safety related information is available [136]
3. Display safety related text messages
4. Work as "navigation aid" to guide the person to to safe areas (muster stations, shelters, emergency exits)

For this purpose, a pager and a smartphone like communicator were designed and implemented within the work for this thesis:

3.3.2 Pager

The messenger or pager device is a small unit of about 60x40x20mm size which is covered by a textile pouch and attached to the clothing of the person by a snap hook or attached to the belt (picture 15).

Picture 14: Pager inside charger

Picture 15: Pager device in pouch

The unit hosts a LiIo cell like the one used in the ISBP1 battery packs (chapter 3.2.4.1), a wireless LAN "System on Module" with microcontroller ("PIC" based) to host small application programs and a dot matrix display.

As the device is used in one of the most hostile working environments underground, the pager does not have any external electrical contacts. Charging of the device is performed via an inductive power transmission between the charging station and the device. Picture 14 shows the pager inside the charging station.

This device was completely designed to meet the following safety support functions [12]:

1. It provides an alarming capability by an acoustic and visual alarm. For the optic alarm, the display background color turns to red instead of the regular green color.
2. Via the Wireless LAN its location can be tracked throughout the mine in WLAN covered areas
3. The user is able to actively send and receive operational and safety related messages
4. The user is able to trigger a distress call (alarm)

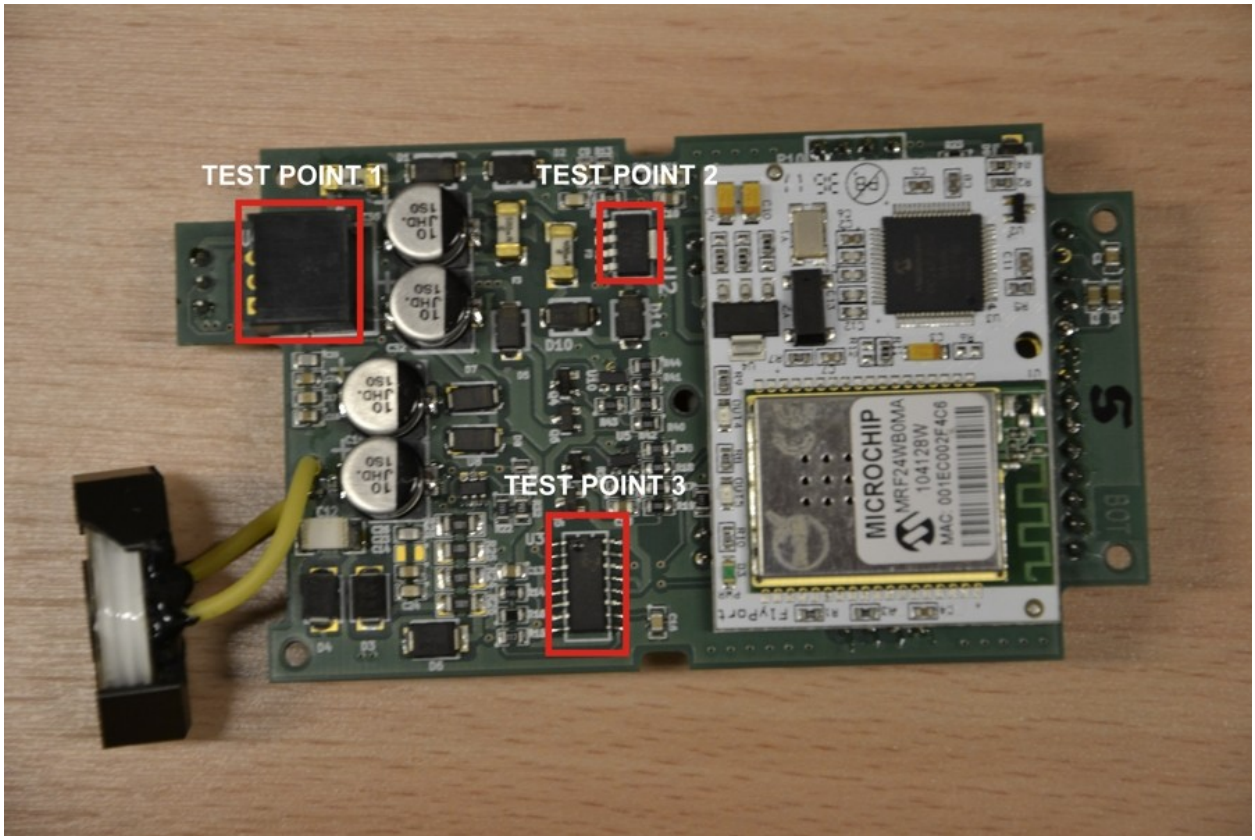
As a System-On-Module, a "*Flyport*" module [131] [157] is used which hosts a WLAN system module from Microchip [157]. This module is mounted on a small base board hosting the power conversion, charge controller and inductive power transmission. Additionally, the device

has a built in MEMS gyro for future use in the Safety Support system.

Especially the inductive power transmission was subject to extensive testing during verification of the design. The function had to assure charging the cell (Panasonic CGA 10446) [134] above ground in less than 6 hours in order to allow the pager being used again in the following shift, which is no problem as the inductive power transfer provides up to 8W to be transferred .

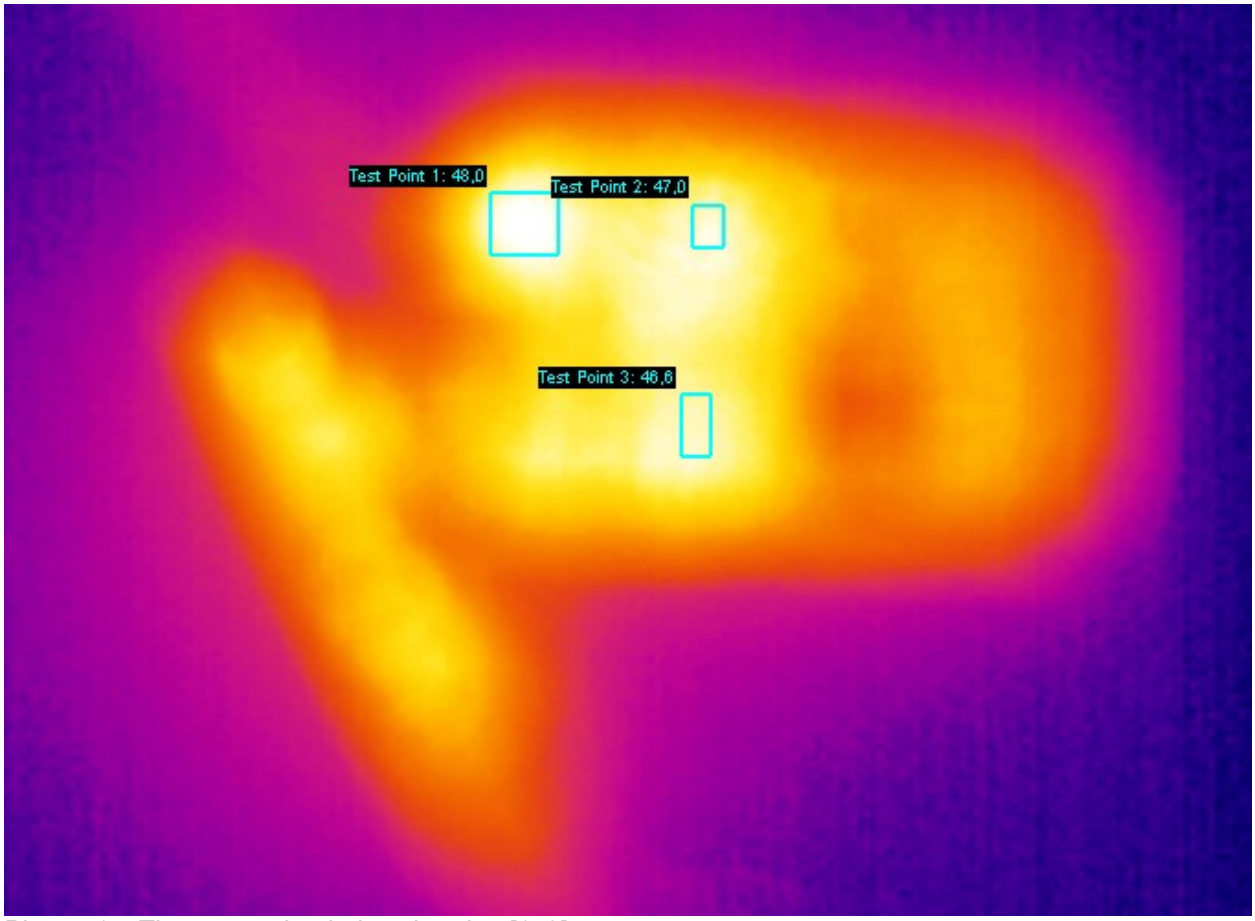
To assure a smooth overall function, the related charger was designed directly in conjunction with the pager device itself. Charger and inductive transmission modules are in identical form used for the Smartphone device (chapter 3.3.3).

The assembled PCB (picture 16) is together with the battery assembled inside a custom made plastic housing. To enhance WLAN performance, a separate antenna is mounted inside the enclosure instead of the PCB antenna on the Microchip module. After assembly and test all device is encapsulated by silicone compound after which the cover plate with the laminate keyboard is mounted in the top of the casing.



Picture 16: Pager PCB with test point markings for thermography [140]

As all devices, the pager PCB also is tested in a thermography in different use cases. The thermography shown in picture 17 represents the use case for charging the unit with the

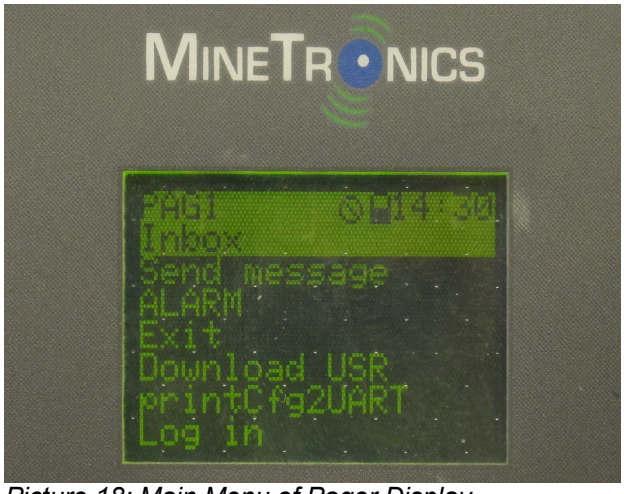


Picture 17: Thermography during charging [140]

measurement points as indicated in picture 16 [140]. All these points concern the power conversion (DC converters and charge controllers) and are max. 20K above ambient temperature.

During software design for the unit it showed that the memory resources on the controller are very limited for the extended functions needed. Therefore, a second revision of the base board hosts additional memory chips connected to the Flyport module via an I²C bus.

The software is set up to accept a number of downloaded messages from a central server ("*PagerCenter*", see chapter 4.1). These messages are accessible for the user via the keyboard / display user interface (picture 18), where the user simply selects those from the downloaded list of messages. These messages are consisting of three groups [12]:



Picture 18: Main Menu of Pager Display

1. Safety related messages (available to all underground workers)
2. General operational messages (available to all underground workers)
3. Work specific messages (available to a specific person or to a group)

Upon reception of a message, the unit warns acoustically and optically by switching on the background illumination of the display. The person can read the message on the display and scroll using the up/down arrow keys. If the message received requires an answer, the message sent may contain a section in the end of the message that contains prepared answers ready to be sent upon selection by the user. This can be a simple acknowledge ("*Yes*"), a negative acknowledge ("*No*") or any other message text. If prepared in the response template also a parameter can be selected by the arrow keys (e.g "*ready in n minutes*" with the number *n* being selected by scrolling up/down). This way a simple user interface is created without requiring an alphanumeric or at least a numeric keyboard [12]. Another advantage of this solution is that the answers can be processed electronically enabling the fully automatic work order handling by interpretation of a "*done*" message and automatic creation of the daily work reports.

The pagers have to be centrally coordinated by a *PagerCenter* server computer (see chapter 4.1).

3.3.3 Phone and Communicator

Another crucial device for Safety Support networks is a mobile voice communication device which at the same time is able to run applications providing Safety Support functions in the underground working environment [95].

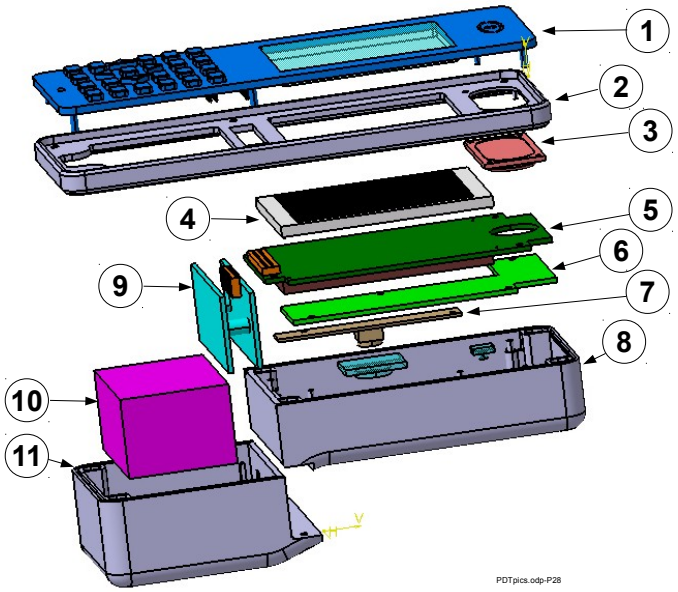
Partly basing on components and technology used in other products like the inductive charging and the LiIo battery and in the same philosophy of using market available system-on-module components a mobile VoIP phone was designed to meet the demands on a versatile multifunctional underground communication device.

This device also bases on an open platform system-on-module ("*IGEP*") [71], a 68x18mm assembled PCB with module plugs on the lower side. This module hosts an OMAP processor, up to 4GB RAM, 4GB Flash and Bluetooth and WLAN transceivers [71].

Picture 19: IGEP System-On-Module (1:1) [71]

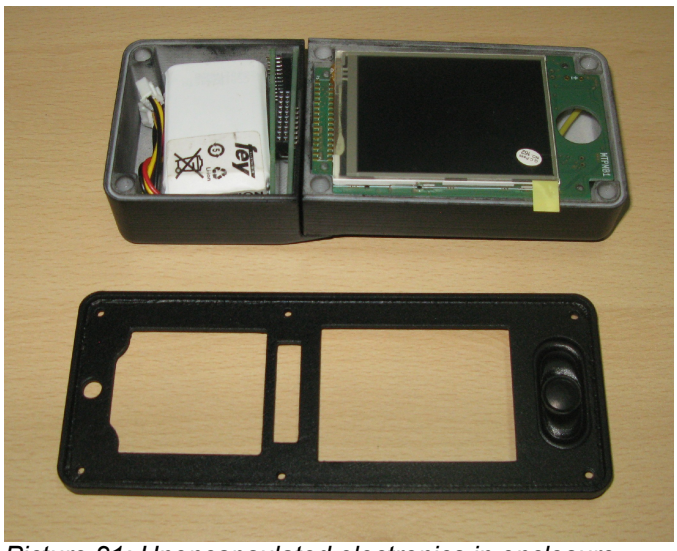
Around this module two PCB's had to be designed to host the phone's functionality (picture 20). For simplicity reasons and to enable a testing with reasonable effort in small production series it was decided to design these PCB's as double layer boards which prove to be a big challenge for the PCB design:

1. The Baseboard for the CPU module (No. 5 in picture 20) which on the upper side hosts the full color 2,8" QVGA display
2. A PCB hosting auxiliary functions and the inductive power receiver and power conversion parts (No. 6)



Picture 20: Mechanic Design of phone

Together with an additional and optional USB camera module (No. 7) mounted underneath the power conversion PCB the electronics is mounted inside an custom designed injection mold plastic enclosure (No. 8). This part of the enclosure is connected to the separate battery pack via the keyboard (No. 1) which also acts as a power conductor to the separate battery pack via connectors on the main PCB (5) and the battery pack PCB's (9). This separate set of two small PCB's inside the battery pack was designed mainly to host the safety functions for the battery pack (No. 9) [100].


Picture 21: Unencapsulated electronics in enclosure

An additional MEMS gyro on the power preparation PCB (No. 6) is not actively used today but will be very useful for the Safety Support functions of this device in the future [95].

Also the phone is not equipped with any external electrical contacts. Charging is performed inductively via the rear of the enclosure when the unit rests in a specifically designed charging bay. This charging bay is designed in the same footprint dimensions so it can be placed aside with the dual pager chargers (Chapter 3.3.2). The power supply also is identical (48VAC), which makes it possible to use the chargers connected to a related power bus bar [95].

Picture 22: Phone in Charging Device

Testing of the hardware was performed especially with the focus on power consumption and battery lifetime [97] as well as on the thermal behavior of the device [139] as well as about the acoustic performance [94] and detailed functional testing.

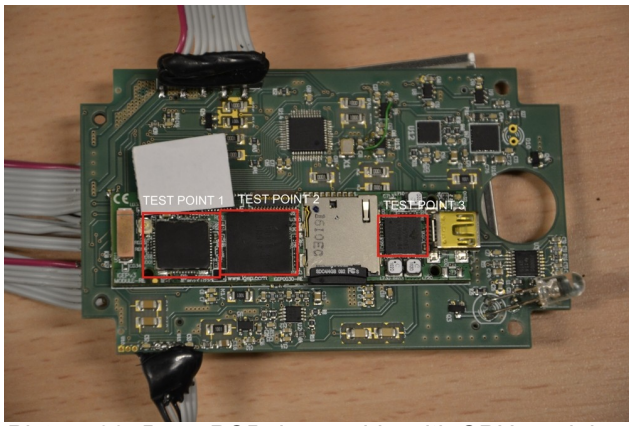
Especially the power consumption testing was carried out extensively. The overall result is that the phone consumes [97]:

Idle:	2,3 W
Ringing:	5,6 W
Talking:	3 W

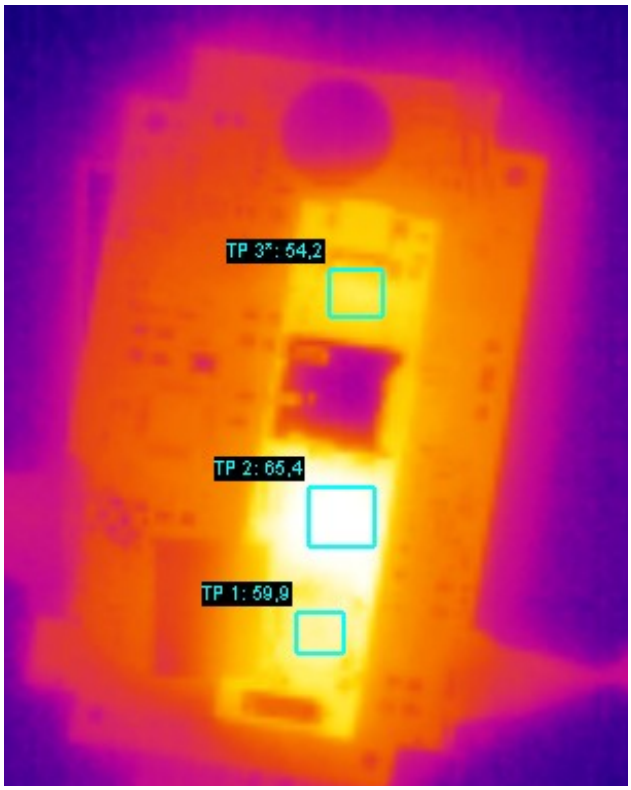
Taking into account a usable capacity of the battery of about 10 Wh this would result in a battery lifetime of 10Wh / 2,3W = 4,34h. This value is too low and does not match the design targets of 8 hrs. The cause for the high consumption was found in the WLAN chipset used by the IGEP module: Taking into account that in idle mode no other components than the IGEP CPU module are active this value is much too high compared to the specification of the IGEP module, which states an idle current of 80mA and a max. current of 450mA at 3,8VDC supply voltage [71]. Taking into account that the device in most of the time will be idle, an average consumption for the IGEP module of 3,8V x 0,1A = 0,38A was calculated during design. Together with the devices around and power losses a usable time of 8 hours equaling 10/8=1,25W should be feasible.

At the time of writing this thesis the source of the problem has been found in the driver of the WLAN chipset used which is currently being fixed. Due to another delay caused by the obsolescence of the display also the display driver needs to be updated.

The temperature testing was performed for the PCB's. The worst case situation is shown in picture 24 where the CPU board is shown running on 1GHz CPU clock and with WLAN under full load. The resulting temperatures on the CPU are 65,4°C (43,4K over ambient) and 59.9° (respective 37,9K over ambient). Running the device on these conditions however is highly improbable even if the values are fully within the margins of the certification. Also in this device, hot spots will be propagated well through the encapsulation compound [100].



Picture 23: Base PCB: lower side with CPU module



Picture 24: Thermography (WiFi ,1GHz CPU) [139]

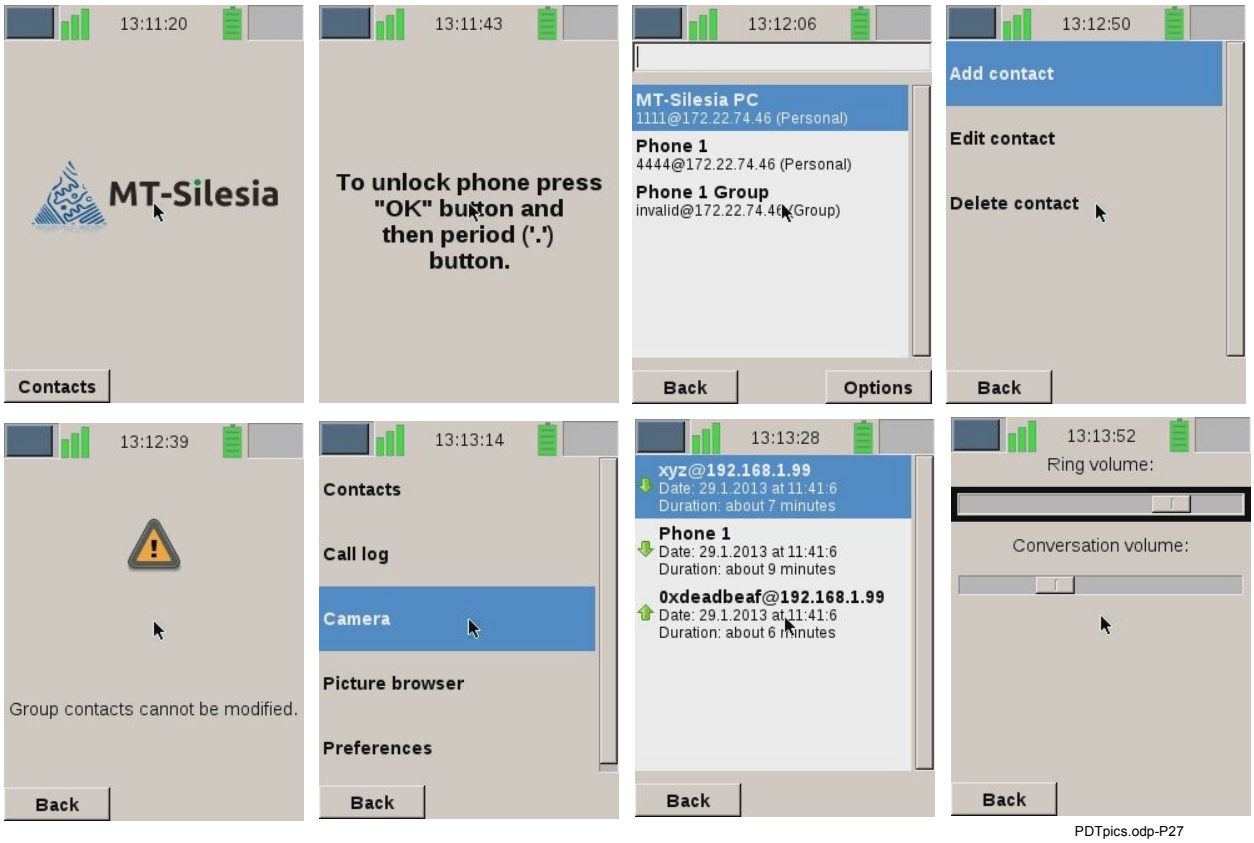
Under the first tests with ready prototypes a slight warming of the device could be observed which is in connection with the excessive power consumption of the WLAN chip [97].

Hardware testing of all other functional devices like camera and MEMS gyro has been successfully completed as well as the testing of the main microcontroller (AVR32) handling the general device logics and the keyboard as well as some internal general Inputs and Outputs for e.g. a flash LED for the camera and an optic call signalization.

The functional design of the basic functions of the device are finished. As operating system, a LINUX derivative supported by the IGEP manufacturer incl. their board support package is used [71]. However this also had to be extended by attaching additional hardware like the keyboard and the MEMS gyro to the system.

The user interface is kept as simple as possible in order to allow usage in the mining environment. This was also the driving factor for the traditional design of the device with

laminate keyboard rather than using a touch screen which is hard and inconvenient to operate with working gloves. A selection of screen shots is shown in picture 25.



Picture 25: Selection of screen shots MTP1 phone

The operation principle follows well proven traditional mobile phone procedures. Selection of items is performed via the arrow keys, confirmation is given using the middle "OK" button. Two context sensitive functions are implemented individually for a specific screen with their respective function shown on the screen (see "*Back*" and "*Option*" buttons on picture 25).

As the pager / messenger device also the phone is prepared to be used in a user independent way with a personalization performed upon a user taking a device from a charging rack prior to use [95]. This principle required different configuration levels to be implemented:

1. Basic Device configuration containing calibration and configuration parameters for the individual device
2. Configurations for the group of workers the person belongs to (phone book entries, software configurations)
3. Individual settings like call lists etc.

Those settings are to be uploaded to the device when the user has identified himself at the time a device is taken for use.

3.3.4 Mobile Machine Communication

In some applications when e.g. operating machines, a personal mobile communication is not suitable or not required as the machine can be equipped with fix mounted data and voice communication units which allow tracking and the exchange of safety relevant information.

For machine data communication, the "*Mobile Machine Gateway*" ("*MMG*") device is set up basing on the hardware of the stationary network nodes (*MIC* see 3.2.3) in order to make use of hardware and software platform commonality. As a derivative of the stationary network nodes these devices are built up identical to the Mining Infrastructure Computer modules, but without any fiber optic switch installed inside. Thereby they are ideal to be mounted on mobile machines [10].

In terms of safety support, for driver communication a dash mount unit shall be available providing the functionality explained for the Personal Communication devices in chapter 3.3.1. However certain functions may not be available (as the guidance to a safe place) as the unit is fix mounted on a machine which most probably may not be used in an emergency case.

Picture 26: Mobile Machine Gateway

Any of these devices has to be capable of seamless roaming for a non delay handover between the access points, which is implemented using the monitor mode of the WLAN transceiver without the need for any special implementations on the access points.

3.3.5 Man, Machine, Material and asset tracking

This chapter explains the functionality of the tracking solutions as defined in chapter (2.4.1). As these functions are related to the location detection of field devices they are handled in this chapter however their implementation in this system mainly is performed in the network nodes (3.2.3) in order to allow any kind of WLAN devices to be tracked. On the other hand, certain devices may also produce their own location data, e.g. dependent on the use of device

internal navigation components (like distance counters on trains or built in MEMS gyros in handheld devices [95]).

Tracking is a typical example for a functionality which adds value for both safety and regular operation. Consequently in this system tracking is regarded as a generic function regardless of it's use for safety related purposes (e.g. man tracking) or for operational purposes (as e.g. material tracking).

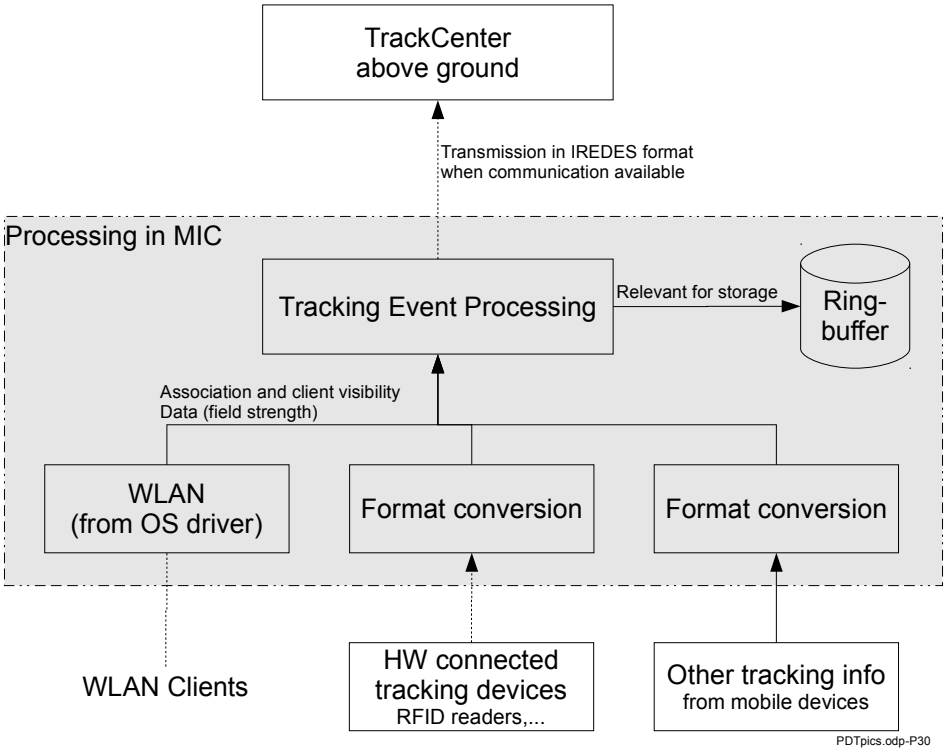


Figure 19: Processing of different tracking information sources in MIC

The implementation of the tracking services therefore has to take the versatility of three different information sources into account:

1. Location information of WLAN client devices worn by people or mounted on assets like machines or vehicles which are generated by the stationary MIC network nodes by interpretation of the signal properties of WLAN client devices within coverage range (see 3.3.5.1)
2. Location information generated by raw data incoming from dedicated stationary mount devices like active or passive RFID readers which are connected to a MIC network node (see 3.3.5.3).
3. Location information completely generated and sent by mobile devices which are equipped with electronic capabilities to generate their position within a mine like e.g.

distance counters on vehicles or trains or Inertial Navigation Systems used on machines (see 3.3.5.4).

Depending on the channel (1-3) the tracking data is reaching the next MIC network node, the incoming data has to be converted and / or interpreted to unify the processing inside the MIC: If all mine workers are equipped with any WLAN based personal devices like man tags, messengers or phones (see 3.3.1ff) a related software on the MIC's within the "*Intelligent Infrastructure*" (3.2.3) is able to detect the associated wireless devices and send a resulting message to a central server as soon as the device is connected to the MIC or as soon as the MIC has the device within its range of coverage.

Within this functionality the MIC may be configured to store a certain type of tracking information (as e.g. all personnel tracking) locally on the MIC beside sending it to a central server. This local storage is required for all tracking information of potentially local safety relevance such as the locations of people or transport vehicles which potentially can be helpful during self-escape. The type of items of potential safety relevance to be stored on the MICs have to be configurable within the MIC's safety support system parameter set.

Thereby the server above ground ("*TrackCenter*") always is informed about the location of the people in order to help efficiently managing and conducting SAR operations in an emergency case: Once the connections to underground systems are cut, the server always can provide a full picture of the situation immediately prior to the connection loss.

This function is implemented for any WLAN device in the MIC [116]. The personal device does not need any dedicated software for this functionality. When the device has been personalized statically or prior to the person going underground, a specific person can be identified together with his / her location under ground.

Especially for operational reasons of a mine it is important to know where assets, material and machines are located. Therefore, the same tracking system also may be used for different items to be tracked using WLAN or even different technology to identify a specific item at a specific location under ground. This may be applicable e.g. to RFID based system (3.3.5.3) to track material or assets in the mine. From the MIC point of view, all such data is handled identically: The MIC receives the tracking data and sends it in unified XML WebServices packets to the TrackCenter above ground. This data exchange has just been standardized within the international IREDES standard [70].

3.3.5.1 Tracking using WLAN signal data

The use of WLAN signal strength information in tunnel environments is no perfect way of acquiring position data from mobile computing devices. For use in buildings and free space there are some systems available for generation of location information by the use of signal strength and S/N ratio from different access points [52]. These systems base on the principle that many access points are located in different distance and in different angles off the client device to be positioned, as timing based systems are not possible with WLAN technology [52].

However in a tunnel, three factors prevent this principle from working efficiently:

1. In a tunnel, the access points for physical reasons have to be aligned along the tunnel line which results mainly in very small angles in between the client device to be tracked and the access points used as fixpoints to generate the tracking data.
2. Only few access points (typically max. two or three) are visible from one single client device.
3. The characteristic signal propagation in a tunnel does not allow an unambiguous use of the attenuation curve for exact determination of the client device location [105][104] [107][5].

Especially the signal propagation of WLAN is a very implementation relevant issue not only limited to tracking but affecting all use of Wireless LAN in tunnel environments. Therefore, this fact shall be discussed more in detail by evaluating a typical attenuation curve from a straight underground tunnel as shown in figure 20.

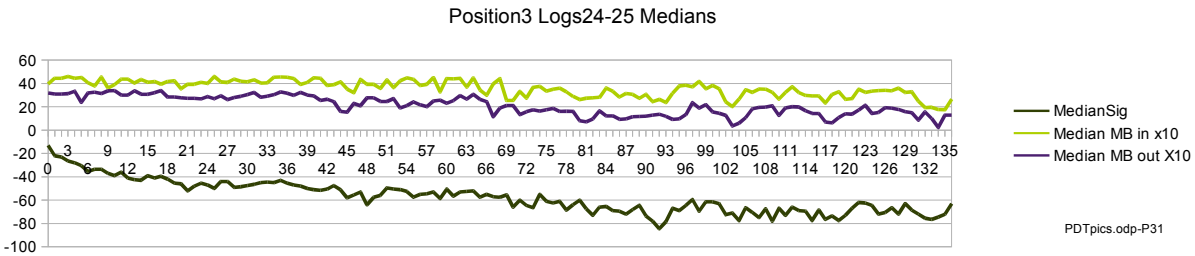


Figure 20: WLAN behavior over distance in meters; Premogovnik Velenje 2012 [105]

The curve in fig. 20 clearly shows that it is not possible to assign one single position (x-achses) to one specific signal strength value making positioning by signal strength impossible. All measurements in straight underground tunnels also confirm that there are wide areas where the signal strength nearly remains within a very narrow horizontal band over wide distances. This

fact can be explained with the fact that the electromagnetic waves in a tunnel create some kind of a "waveguide effect" [155][35][83][72], which lets the tunnel itself behave similar to a coaxial conductor in which the multiple reflected signals "guide" the usable signal over a long distance. This effect is determined by the tunnel size (cross section) and the operating frequency [155], a fact which also can be experimentally confirmed by a large number of WLAN site surveys carried out by the author and his team as e.g. in [105][107][5][104].

Figure 21 shows another example of a measurement performed in a long straight tunnel of not optimal cross section disturbed by a conveyor belt system installed throughout the tunnel. Nevertheless, the usable signal in this constellation reaches about 350m [105].

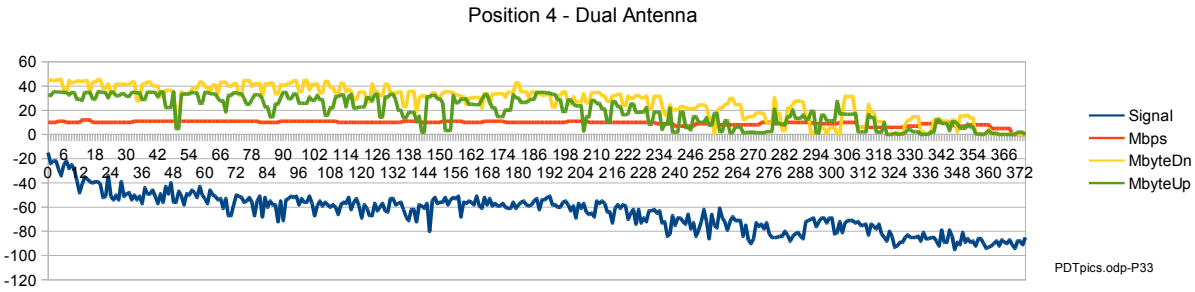


Figure 21: WLAN throughput and signal versus distance with antenna diversity [105]

In this examples, three sections of the signal attenuation can be identified, which in principle are identical to what Sun explained in [155]:

1. The near field at the antenna up to about 30m - 40m from the stationary antenna. This section is determined by a attenuation curve close to what can be expected in free field distribution.
2. The waveguide area from about 30m - 40m onwards up to about 200m from the stationary antenna. This section is determined by a more or less constant signal strength in between -50 and -70dBm, where a very well usable communication is possible.
3. The volatile area at the end of the coverage range, where the signal strength falls below the usable values. This area is not visible in fig. 20 as the measurement finished before the end of the coverage was reached, which is clearly visible by the fact that there still was a netto throughput of 2 Megabyte per second measured.

From these circumstances, the relevant points for interpreting WLAN signals in tunnels for functional implementation of tracking and communication applications are derived in figure

22. These findings are now taken into account in the design and implementation of underground WLAN applications.

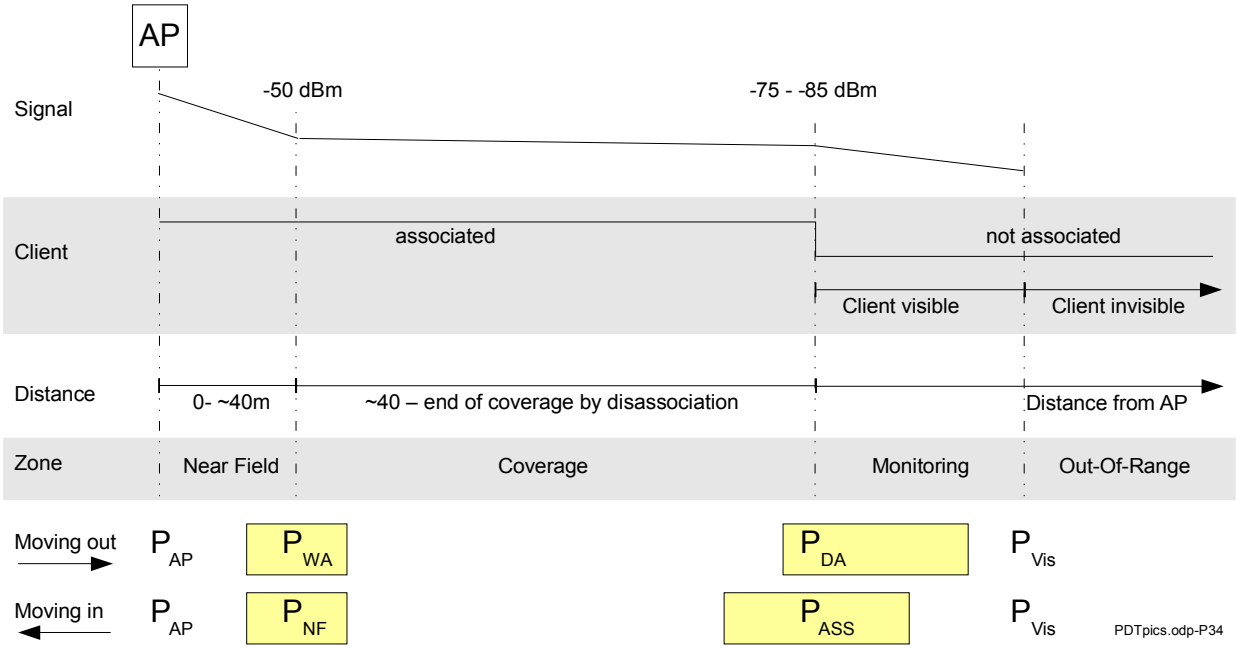


Figure 22: Implementation relevant WLAN working areas and set points

As the exact location of some points may vary significantly depending on the moving direction of the client (towards and away from the access point), their names change with the moving direction. The colored area around these points indicates the zones around those points and their tendency. The location of P_{DA} and P_{ASS} also strongly depends on the availability of an accesspoint on the far end of P_{AP}: If a connecting access point is available P_{DA} may be located much closer to P_{AP} than without a connecting access point available.

P_{WA} and P_{NF} are not relevant for regular WLAN communication system design; They only have an importance when special near field applications have to be implemented (as the WLAN gate application described below).

Taking these results into account, a positioning and device tracking application using the Wireless LAN signal strength data can reliably only be implemented in the following way:

1. By association of a client device to a specific access point: If the device is associated with the access point the location of this particular client device is within the usable coverage range of this access point. The device is located between P_{ASS} on one side of the coverage and P_{DA} on the same or the opposite side of the access point coverage. This is the standard mode as used on the MIC network nodes which resulted from this thesis' work (3.2.3).

2. By application of a near field identification in the signal strength interpretation: If the MIC receives the client signal with a signal strength value higher than -40dBm, the client device most probably must within about 30m off the MIC antenna. This filtering can be set quite reliably as such high signal strength readings are excluded in the sections further out from the stationary antenna. In this case the device is located in between P_{NF} and P_{WA}.
3. By implementation of a far field recognition in between the points P_{DA} and P_{VIS} (or P_{ASS} when returning) which in continuous coverage situations will result in the fact that the client device is already associated with the next access point, but still visible at the current base station. This filtering however can be very unreliable as the far field in practice cannot be reliably identified by some signal strength value threshold especially in situations when the tunnel cross section temporarily is disturbed by e.g. machines or vehicles moving through the tunnel. The only applicable implementation for such a far field section is to assign a status where the client is visible but too far for associating or data communication.

3.3.5.2 WLAN access control gates to dangerous working zones

A further implementation of WLAN based tracking is a special application of access control gates, which is performed in one particular mine in order to register which people are inside or outside a potentially dangerous working zone. As a MIC has two WLAN interfaces available for use, one will be used actively for communication. The other WLAN interface is available e.g. for use in a monitoring mode for detecting client devices in a kind of electronic gate formed by two directional antennas which are oriented in an anti parallel way in the tunnel, whereas both antennas are connected to two different antenna ports of the same transceiver (Fig. 23). Both antennas are located in the tunnel such as they create three coverage areas characterized as sectors in fig. 23:

1. One sector where only antenna A1 receives the signal from a passing client
2. One sector where both antenna A1 and antenna A2 receive the signal from the passing client
3. One sector where only antenna A2 receives the signal from a passing client

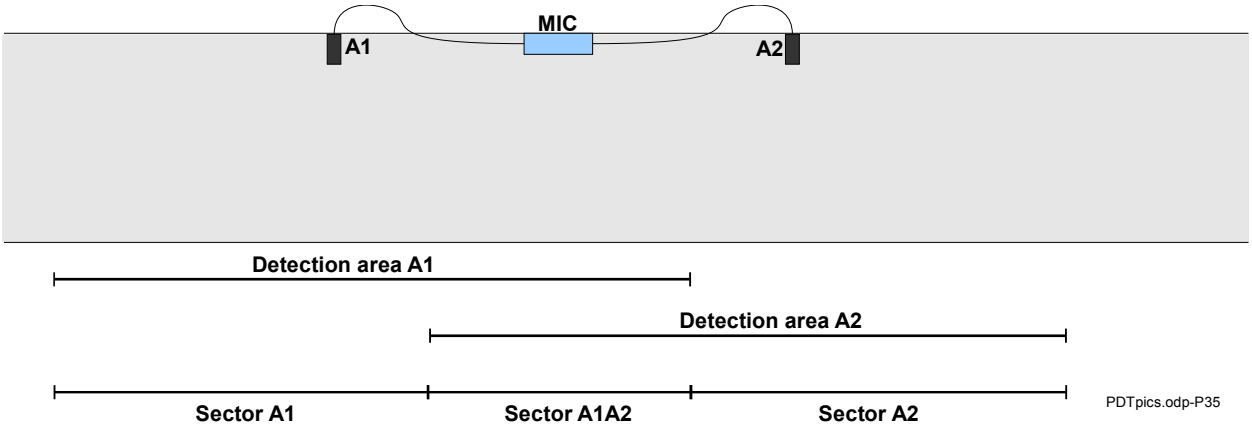


Figure 23: WLAN access control gate setup

As the entire application runs in the near field area (in between P_{AP} and P_{WA} acc. to figure 22), all signals above a certain field strength are used while all signals below can be ignored helping to limit the areas in a sufficient way in practice.

The signals are interpreted in accordance to the following decision table:

A1	A2	Client in Sector
-	-	none
-	X	A2
X	-	A1
X	X	A1A2

When a person moves through the gate, the following transitions according to table 1 determine the detection of people moving through the gate into the direction of the dangerous zone (from left to right in figure 23). A precondition is that the person's tag at the time of first registration in the gate is not registered as present inside the dangerous zone:

Ti1: The person moves into the gate and gets initially detected by the first gate antenna coming from the left. Due to the fact that the tag is not registered as inside the dangerous zone and neither registered by another antenna in the gate the incoming direction is defined.

Ti2: The person moves further into the gate (into zone A1A2) and is now detected by both antennas.

Ti3: The person leaves zone A1A2 and enters zone A2 where the tag only is detected by antenna A2.

Ti4: The person tag is invisible by the gate antennas. As it was not registered in the beginning and has been registered by at least antenna A2 while walking through the gate, the person now is regarded and registered as "*inside the dangerous zone*"

(“*InDZ*”).

From	To Invis.	To A1	To A1A2	To A2	To InDZ	Remarks
Invis.	-	**Ti1**	**Ti2**	**Ti3**	TEi1	
A1	**To4**	-	**Ti2**	**Ti3**	TEi2	
A1A2	TEo3	**To3**	-	**Ti3**	TEi3	
A2	TEo2	**To3**	**To2**	-	**Ti4**	
InDZ.	TEo1	**To3**	**To2**	**To1**	-	
						Legend: **Invis.** Tag **inivis**ible and not registered as **InDZ** **A1/A2** Zones **InDz** Tag counted electronically as **in**side **D**angerous **Z**one (right of A2)

Table 8: Transitions in RF access gate

In identical form the detection of the outgoing persons is performed. An outgoing person is defined as wearing a WLAN tag which before entering the gate is electronically registered as “*inside the dangerous zone*” in order to be able to detect the outgoing direction.

This four stage process assures a highest possible reliability of the RF gate, however it never can be determined accurately how people wear the tags which is decisive for the functioning of the gate. Therefore, a number of error conditions can be detected. Missing a detection in the first or in the second zone while walking through the gate can be automatically healed by the gate itself, which is shown in the yellow fields in table 8: Being directly detected in zone A1A2 from the invisible stage is regarded as having been detected by A1 before. The same relates to coming in to A2 directly from the invisible stage or from A1.

Special attention therefore is needed for the errors which occur on the last detection step as it cannot be excluded that a person inside the gate changes direction and walks back to the direction he came from. For the incoming passage these are the errors TEi1 – TEi3: In all these cases the last detection of A2 is missing which makes the person “hanging” in the gate

TEi1: Person moves directly from “*invisible*” state into the dangerous area without having been detected at all. This error needs to be prevented by operational measures like how people wear the tags and by careful maintenance of the gate and especially the antennas and their orientation.

TEi2: Person has been only detected by A1 and became invisible after that neither having been registered in zone A1A2 nor in zone A2, which means that the person returned to the safe area (turned back to the left in fig. 23). If the person moved on into the dangerous zone, both detections in A1A2 and in

A2 are missing. This error is like TEi1 the most dangerous one in the gate and needs to be prevented by operational measures like how people wear the tags and be careful maintenance of the gate.

TEi3: Person has been detected in Zone A1 and A1A2 or only in A1A2 and the tag becomes invisible without having been registered neither with A2 nor with A1. This is interpreted as "worst case" in terms of safety meaning that the person is inside the dangerous zone as the movement direction was clearly identified by the incoming sequence. However the lack of the final confirmation of the person's status is visualized on the ViewCenter software (chapter 4.1).

TEo1: Person moves through the gate from the Dangerous Area to the Safe Area without having been detected at all. This error is by far not so critical than the matching TEi1 where the Dangerous Area erroneously can be reported safe and clear of people.

However in all TEo cases the final security that people are outside the area always can be electronically detected when the people after the shift put their man tags or WLAN client devices into the charger stations above ground which is the ultimate security that they have left the area.

TEo2: The leaving person was detected by A2 but not detected by A1A2 and A1 before becoming invisible. This means for the electronic interpretation that the person turned around and went back into the Dangerous Area, which matches the interpretation of transition Ti4.

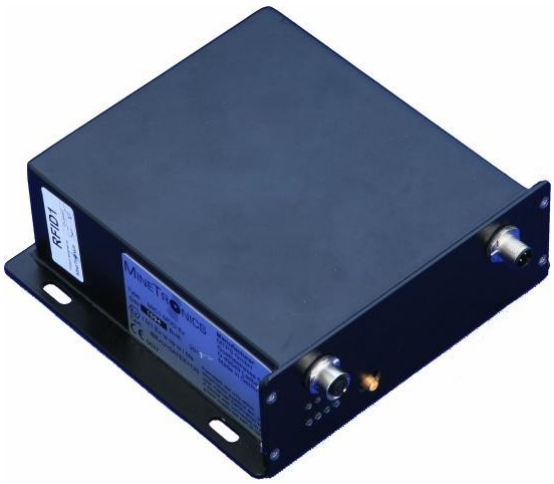
TEo3: The leaving person was detected by A2 and A1A2 but not in zone A1 before the tag became invisible. This case is interpreted that the person left the dangerous zone as the movement direction was determined by the move from A2 to A2A1. However the lack of the final confirmation of the person's status is visualized on the ViewCenter software (chapter 4.1)

The gates application is implemented on the related MIC with all functions concerning the interpretation of the antenna signals. The related zone information is then sent as a regular tracking datagram to the *TrackCenter* central software system (see chapter 4.1). As these gates are installed at every single access tunnel to the dangerous area, the interpretation of the transitions and the people inside and outside the dangerous zone is performed on the above ground Center server. Visualization of the gate is implemented in the 3D mine visualization software ViewCenter.

3.3.5.3 Non WLAN based Stationary Tracking Devices

Stationary Tracking Devices include all non WLAN devices which are installed in a certain location in the mine in order to report on mobile equipment or devices moving by this checkpoint. Such devices are passive or active RFID systems or RF based tracking solutions using communication principles other than WLAN. In conjunction with the work related to this thesis, a passive RFID system was implemented on one mine in Germany in order to optimize dispatch of material logistics and to know where the underground trains are in order to be able to quickly dispatch the nearest train to an emergency location when needed.

For this system, a passive RFID reader was attached to the Mining Infrastructure Computer (MIC) [9], connected to the MIC by a serial line which for intrinsic safety reasons is realized on TTL potential to fulfill the requirements of EN 60079-11 [27]. The passive RFID reader [149] is a board level module. which contains a ready-to-use passive RFID reader detecting passive UHF RFID tags in the 868 MHz band. This module was integrated onto a customized PCB together with custom designed power supply and IS protection circuits [9].



Picture 27: Passive RFID reader module

Picture 28: Passive RFID tag in use on a container

The reader is configured for use via the general Web Configuration of the MIC it is attached to. Configuration commands are sent via the serial interface to the reader module. The MIC also keeps the coordinates of the tag reader in order to be able to assign the correct location to the tracking messages.

Together with an 8dBi antenna connected to it, the reader detects the passive RFID tags certified together with it inside a range of up to 3m. Upon detecting a tag, the reader sends a stream of tag identifications via the serial line to the MIC. The MIC transforms the message stream into one single message for each tag being read at a time.

The data format used for the messages follows the international IREDES standard (*IREDES* = "*International Rock Excavation Data Exchange Standard"*) [70], which is a XML schema based format to exchange all kind of operational and safety related information between different systems in the mining industry. In this case, the recently finished tracking profile is used.

The tracking message is set up precisely in the same standardized format like the data sent for the personnel tags. It also ends up at the same server above ground, the TrackCenter. This method simplifies setup, communication and processing of tracking data for any purpose in the mine.

In the same way also tracking data from other devices is processed which are directly connected to the MIC, like data from proprietary tracking systems built into cap lamps working with active transmitters on an UHF or 2,4GHz band.

3.3.5.4 Position data from mobile devices

Some mobile equipment underground is able to compute their own positioning information as e.g. a train locomotive or a remote controlled loader [170]. These machines use distance counters on the wheels (locomotive) or distance counting together with laser scanner based navigation (loader) to determine their location in the mine.

In addition, also the MineTronics developed handheld devices ([95][12]) are prepared for a basic direction and location finding by their built in semiconductor based MEMS gyroscopes.

Such devices can send their position information to the network where the packets are taken by the closest MIC which if necessary transforms them into the IREDES standardized format and forwards them to the TrackCenter in order to have all location based information in one single database which also enables the system to inform Miners (e.g. by messages to pagers or opto-acoustic alarm of their personal devices) that a machine or a train is approaching to minimize danger of collisions.

3.3.6 Accurate Positioning applications

The tracking via network and WLAN technology only provides a rough overview of the locations of people and assets with a minimum accuracy of the association of a mobile device to a specific base station. This is fully sufficient to initiate and conduct search and rescue operations

and to assure that certain areas are clear of people.

For certain applications like collision detection a potential extension of the tracking system is the optional application of positioning devices using e.g. time-of-flight measurement techniques to accurately position people and machines. The base stations of these devices can be assigned to or integrated with the MIC in order to allow access via the network.

Such systems are e.g. of importance as safety support sensors inside longwalls where the accurate position of the miners is essential to support safety under ground. Ideally, the positioning systems can also be integrated with sensor networks providing environmental information. If such positioning systems are not used for safety critical sensor information, they may be taken out of operation once the communication system switches to emergency mode.

3.3.7 Environmental gas measurement and ventilation data

In a fully established safety support system, environmental information about gas content in the air and ventilation parameters like air speed, pressure and direction should be known under ground and communicated under ground without any intermediate processing at central computer systems as the central computer systems may be disconnected in case of an emergency.

Therefore, it is recommended to feed all environmental information into the next available MIC as soon as possible so the information resulting from this data will be available to local people under ground during an emergency when all connections to above ground systems are lost.

Due to operational constraints and the requirement of cooperation with a supplier of environmental measurement systems, this integration has not been implemented yet. However, the preconditions are implemented as the required hardware to convert intrinsically safe serial interfaces (mostly RS485 based) into network formats or into a serial interface of the MIC are available. This hardware was implemented in the RSMUX module, which is a cascading input of multiple low speed serial ports to one high speed port of the MIC [90].

Future developments of new underground automation system have to take into account these demands. Once these systems are fully network integrated, a seamless information flow and local use of safety relevant information will be possible. However this cannot be part of the ongoing project.

3.3.8 Semi mobile network extension for temporary and SAR use

In emergency cases the underground network may be damaged as well as stationary network nodes may not be accessible or usable any longer. However, after an emergency rescue teams have to move in to these areas. Also these teams are dependent on communication among each other and with the rescue operation coordinators located above ground or in a preliminary underground location.

This raises the requirement for a semi mobile network extension with transportable active units and related cable. Such a semi mobile network setup conforms of:

- A cable drum with rugged fiber optic cable of abt. 100-300m length
- A switch and an accesspoint built into the core of the cable drum; It would be perfect if a complete MIC electronics could be built in.
- A connection for external (intrinsically safe) power supply to supply switch and accesspoint
- An optional exchangeable battery pack (M1) for independent supply of the active cable drum components

This network can easily be deployed to mining areas which need a temporary coverage. At the same time there is WLAN coverage always around a cable drum which in an optimal situation covers the full area between two cable drums.

This leads to a physical layout of a semi mobile system as lined out in figure 10 on page 70 [115]. This picture shows a cable drum with a large inner diameter required to prevent the fiber optic cable from breaking. The space gained by the big inner diameter is used for fitting a “MIC” communication computer (see chapter 3.2.3) together with a battery backup power supply.

Depending on the construction of the drum, the computer may mechanically reside in the turning part of the drum or in a fixed part if only the outer shell is rotating.

While walking, the armed fiber optic cable from the drum is extended and placed on the tunnel floor. When all cable is used, the drum is simply placed on the floor or hinged on structures in the tunnel side walls.

Before the computer inside the drum is switched on, two WLAN antennas are mounted right onto the connectors in the side surface of the drum. These antennas enable a wireless connection within the WLAN coverage range around the drum. Thereby the Mining Rescue team

has a wireless broadband connection in this area.

When the team continues on its way to the working area, they simply connect the cable end of a new drum to the fiber optic connectors (103 in fig. 10) and roll out the new fiber cable until the drum is empty.

When the rescue team meets a working network, they easily can hook up the preliminary network with the existing underground network via the second fiber port (No. 103 in fig. 10).

In this case, the rescue workers are able to access the information available in the Mining Infrastructure Computers inside the previously disconnected networks, if these MIC's still are powered. This can provides important information to them for carrying out their rescue work, as e.g. the following dependent on the degree of functional implementation:

- Where were the locations of people in the disconnected network segment prior to the active nodes loosing power?
- Network status at the time the emergency was declared (and the emergency mode was entered by the network) together with the locations of people at this time

If the MIC is not powered any longer upon arrival of the SAR team at this point, the SAR team is able to supply electric power to the closest MIC they meet by mobile battery packs in order to download the information about the last location of the workers. As each MIC stores the entire information available in the network (also those locations reported by other MICs), this enables the SAR team to conduct further operation very target oriented:

- Last location of Miners prior to the shutdown of electricity at the node the SAR team accesses first.
- Areas which were actively reported clear of people (no tracking data available and stored in the related MIC). This may be due to the fact that the miners after the emergency gathered together by the help of the system.
- Environmental information of the status prior to electricity shutdown of the MICs.

As the semi mobile network uses identical technical systems as the productive systems, all devices used by the SAR teams can also be used during regular operation and all devices used in regular operation can also be used in SAR operations. This is a fundamental advantage compared to any other dedicated safety communication system.

In detail the SAR team communication functions include:

1. Connectors for emergency headsets (e.g. „*Dräger Mask*“) at each network node

2. Special handsets with connection for built in headsets of emergency masks to enable wireless communication for the rescue workers.
3. For the mobile wireless units optional inputs for personal health monitoring sensors (body temperature, heartbeat etc) for to prevent from exposing the rescue workers to unnecessary personal danger.

4 IMPLEMENTATION OF SERVERS AND FUNCTIONALITY

This chapter explains the implementation of the central systems needed above ground and the functionality of the Safety Support System.

The central server systems are described in chapter 4.1.

All general and system wide implementation of the functionality is described in chapter 4.2. The essential Emergency Mode Detection functional implementation is described in detail in chapter 4.3 before the implementation of the Emergency Mode handling and the related services are explained in chapters 4.4 to 4.6. Finally the realization of the recovery from Emergency mode is described in chapter 4.7.

4.1 Central Server Systems

4.1.1 Overview

The central systems cover all functionality which has to be implemented in above ground computer systems.

The underground network infrastructure and the mining applications provided by MineTronics are all connected to central systems. These central systems are used for administrative and application level purposes. The administrative functionality covers [87]:

1. Providing transparent VPN access to all underground units for service
2. Software deployment to the underground units
3. Configuration deployment to the underground units
4. System debugging
5. Remote configuration and administration of the central systems
6. Remote configuration and administration of the field systems
7. Information storage (Databases)
8. Information analysis

For all equipment explained in chapters 3.2 and 3.3 these functions are provided by a specific server called "*NetCenter*" [87]. As far as possible, the administrative functionality listed is farmost identical for all systems and applications implemented by MineTronics.

The application level functions are dependent on the purpose of the specific application server. In general, an application server system has to implement the following functions [87]:

1. Information acquisition from the underground field devices
2. Application level information storage (Databases)
3. Information acquisition from third party IT systems for integration into the processing
4. Information analysis and processing (Central applications)
5. Information exchange to other IT systems (preferably web based)

4.1.2 Hardware, Operating System and IT Service

It is the goal that each independent application gets assigned one single functional server located above ground. Theoretically, all the servers can be virtualized in order to run on one single hardware machine. However for reliability and system stability reasons these are be split into several hardware systems, which preferably is selected as rack mount PC systems to be mounted in a rack above ground.

The operating system chosen for the general server systems is a LINUX derivative due to it's reliability and cost efficiency for use in server applications. This also provides the possibility to set up fully redundant cluster systems, which are optionally available (fig. 11 on page 75). RAID technology together with solid state disks is preferably used for all storage. In such setup, the cluster servers usually have to be located in a different physical location to provide highest possible amount of physical safety of the overall system availability which deals with safety relevant data in terms of the underground operations.

Complex IT system infrastructures today are very difficult to be maintained in a fully competent way by singular staff on site. In most cases, expert support is needed which is implemented by a remote support system which is integral part of the overall system.

This is implemented via a specific hardware, the "*RemoteAccessClient*" (fig. 11 on page 75), which is set up to provide a singular dedicated port into the network, which can be physically turned on when the mine explicitly allows remote access to the systems. This Remote Access Client uses a virtual private network ("*OpenVPN*") [176], an open source virtual private network system with proven and known reliability [176]. Via this connection a specialist connected from anywhere in the Internet is able to support a certain application provided that he installed the related OpenVPN security certificates on his PC [4][176].

The remote access client at the mine site also provides a separate network interface which is used as a hard wired and potentially also wireless "quarantine network", where suspected defective devices from underground can be connected to in order to be diagnosed remotely without having to disturb the underground network operation [87]. Additional interfaces (like serial ports) may be used in the future to additionally connect special device ports like serial lines or JTAG ports to access microcontrollers on low debug levels if necessary. Also a webcam is planned to be future part of this system in order to be able to remotely see the behavior of LCD displays or indicator LED's. This procedure in most cases makes it not necessary to return

devices to the producer if even deeper problems solely can be solved by software measures.

4.1.3 General Center Server Architecture

Central systems are set up for each of the following applications[119]:

NetCenter:	Network device administration, Network status overview, Handling of safety and normal operation modes...
TrackCenter:	Tracking of people, material and assets independent from sensing technology used
FleetCenter:	Data exchange and analysis for mobile machines
VoIPCenter:	Administration of SIP telephony („Asterisk“) and devices: phones, interkom units, mobile phones
PagerCenter:	Administration of pager devices, user assignment and message exchange according to a new mining standard
SafeCenter:	Handling of all mining safety relevant information extracted from and distributed via the underground networks

These systems have to communicate among each other. For this communication as well as for communication with external systems Web Services are used. The programming language used for the Center Systems is JAVA using the Java 2 Enterprise Edition development environment (J2EE) on the Oracle Glassfish application server [132].

The database interface is kept open to give the possibility to the user of using their own customer specific database systems as ORACLE etc. The default databases used is MySQL accessed by the MySQL data query language.

These demands lead to a software architecture as illustrated in figure 24.

The resulting software architecture (fig. 24) makes one Center Server consist of the following components [22]:

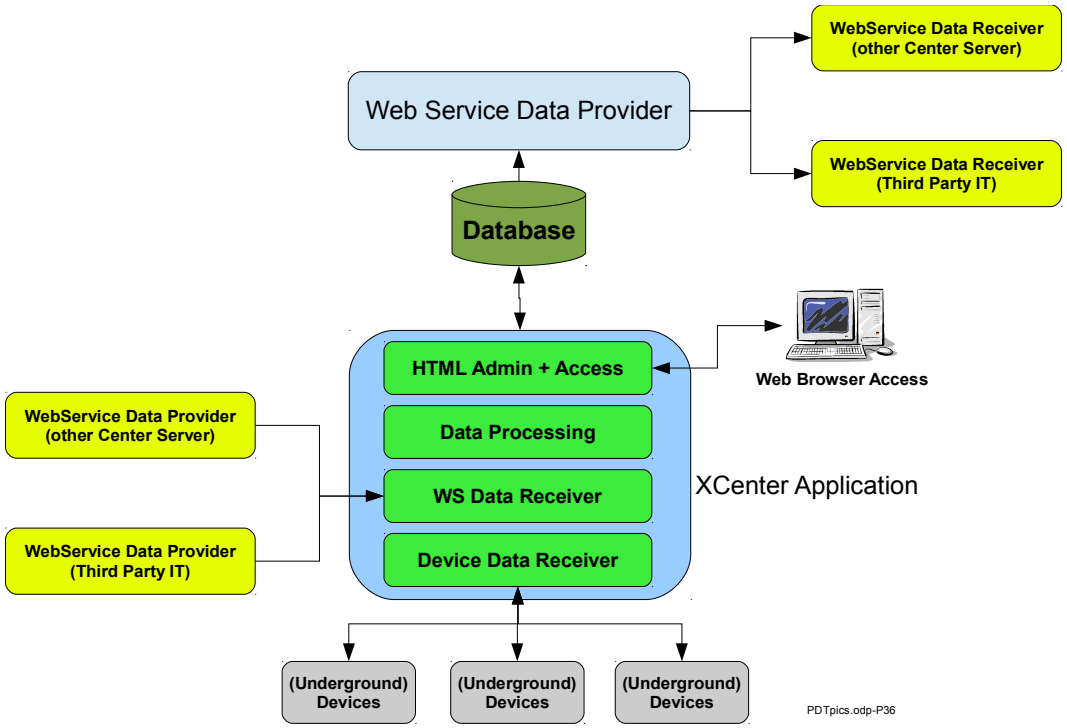


Figure 24: Center Server general architecture

1. A Web Services based Data Receiver component to connect to other Center Servers and to third party Web Services based information exchange
2. Individual Data Interface components for input and output of information to underground devices and all other connected peripherals not capable of handling Web Services.
3. Data Processing Components
4. Database Connectors to an internal or external database
5. Web Service based Data Providers to other Center Servers or to external IT systems
6. Web based administration interface for the related Center Server. This administrative interface also includes user authentication routines to internal or external LDAP servers [145] [169] for user authentication as a single sign on in accordance to RFC4511. In all Center servers, the user roles "*Administrator*", "*Operator*" and "*User*" are implemented representing different levels of access permissions [11].

Whenever possible, standardized interfaces are used. The standard interfaces provided to third party IT systems always are implemented as Web Services [22][119].

The preferred way of internal interface implementation is also the use of WebServices. If this is not applicable for specific reasons, other means may be used preferably basing on XML

structures.

In the following chapters, some implementation details of those Center Servers needed for the Safety Support System (NetCenter, TrackCenter, PagerCenter, VoIPCenter and ViewCenter) are briefly explained.

4.1.4 NetCenter implementation

The NetCenter is the server system which is the basis for administration of all underground network components compatible with the systems explained in this document (see chapter 2.5.2). The NetCenter furthermore stores all network related data which is required to use the network infrastructure for Safety Support purposes [87].

The implementation follows the architecture in figure 24, whereas the devices connected are the active network nodes as well as the handheld units part of the system (smartphone and pagers as well as machine communication devices).

The NetCenter permanently keeps a status overview of all devices underground. This is implemented by the exchange of WebService XML based status messages sent from the devices to the NetCenter server. Beside a time stamp, these status messages include the uptime and important other device information like the number of running processes, CPU load and possible device dependent additional information. The fact that the device answers with the status message as such is the proof that the application software of the device is working [87].

An important functionality of the NetCenter is the network status overview. This implementation is explained in chapter 4.4.1 as it is part of the system wide interactions of the Safety Support functions.

The NetCenter also performs an automated firmware and configuration update of MineTronics produced devices underground. In this way, automatic updates of a number of devices can be performed without requiring a manual intervention. Regardless whether an automatic or manual updated via the web interface is carried out, each device update is performed in the following procedure:

1. The NetCenter downloads the software and a MD5 checksum to the remote device
2. The remote device calculates the MD5 checksum of the firmware target received
3. If the checksum received is not identical to the checksum calculated, this fact is

reported back to the NetCenter in order to restart the transfer.

4. If the checksums match the remote device installs and enables the firmware.
5. During this time the NetCenter (or a remote Web Client if the update was started manually) tries to reach the remote device's web server.
6. When the remote device has completed installation and activation of the new targets (potentially after a reboot), it waits for a new connection from the NetCenter or web browser.
7. If this connection is not created after a certain timeout, the remote device voids the newly installed targets and falls back to it's previous configurations.
8. If the connection is created, the remote device waits for a confirmation ("*Commit*") from the server or web browser in order to finally accept the new configuration and make it the default for future boot and use.

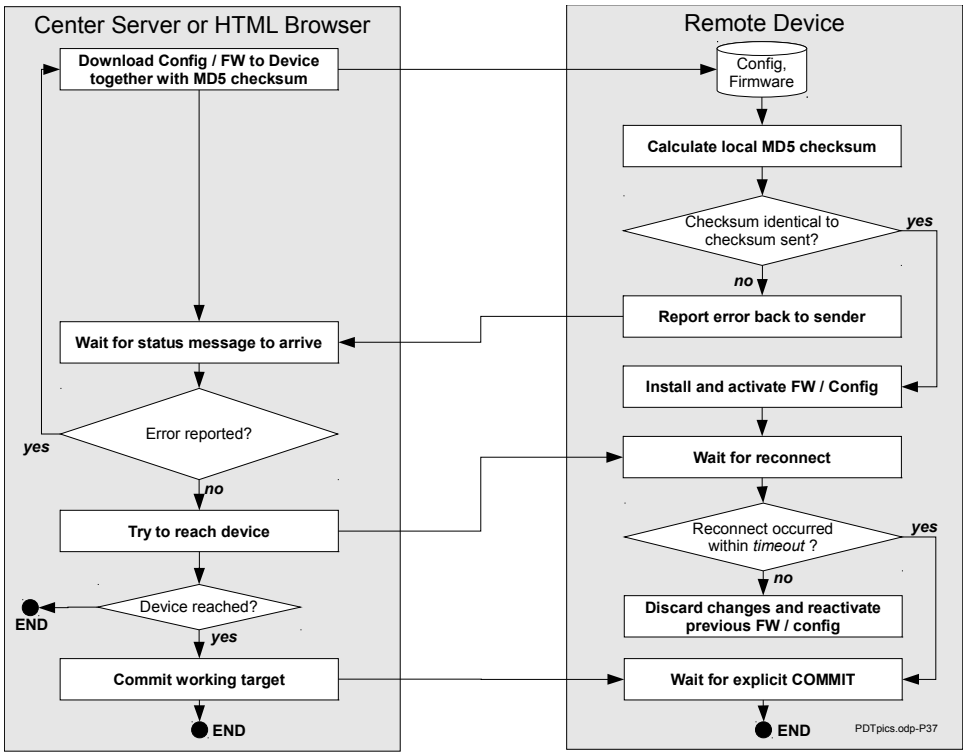
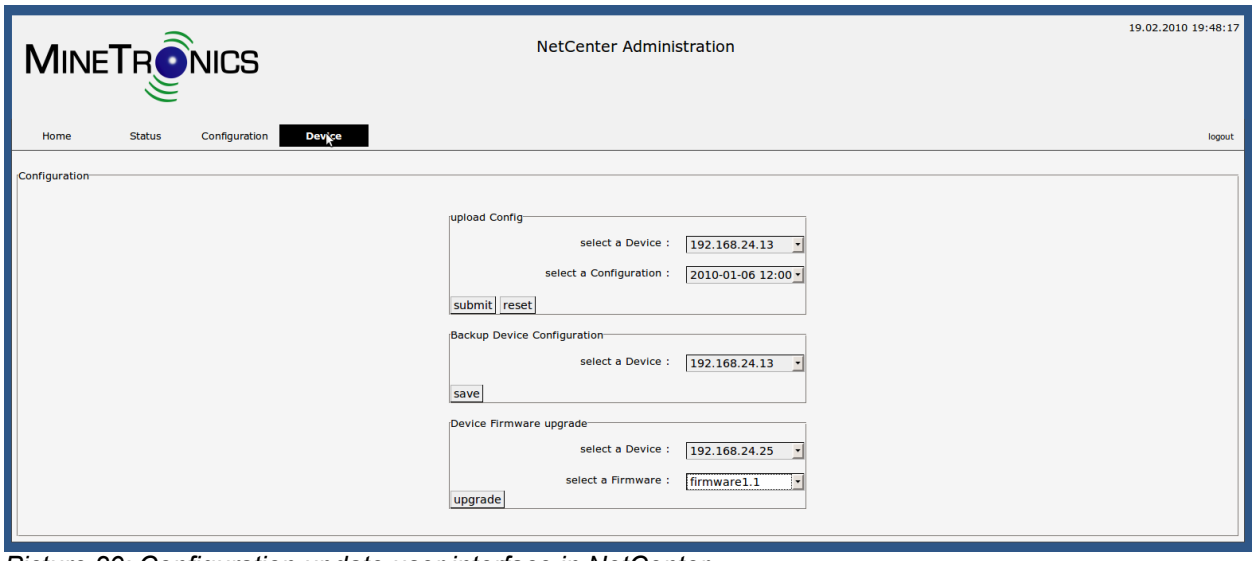


Figure 25: Fail Safe Routine for remote configuration and firmware update

A screenshot of the web interface of the NetCenter for device update is shown in picture 29.



Picture 29: Configuration update user interface in NetCenter

4.1.5 TrackCenter Implementation

The TrackCenter acquires all location information of mobile equipment and people underground from different sources and stores them with time tags in a database. From the sequence of the time tags for one single device the TrackCenter is able to form the track of this person or asset underground. In case of an emergency this makes it the central resource for knowing where people have been prior to an emergency occurred [14].

Picture 30: Track Center Device view in Web Interface

By default, the TrackCenter receives related tracking data packages from the underground network nodes of all wireless devices within range when the tracking packet was generated. When different device connectors are implemented (fig. 24), other proprietary data telegrams from other sources can be integrated.

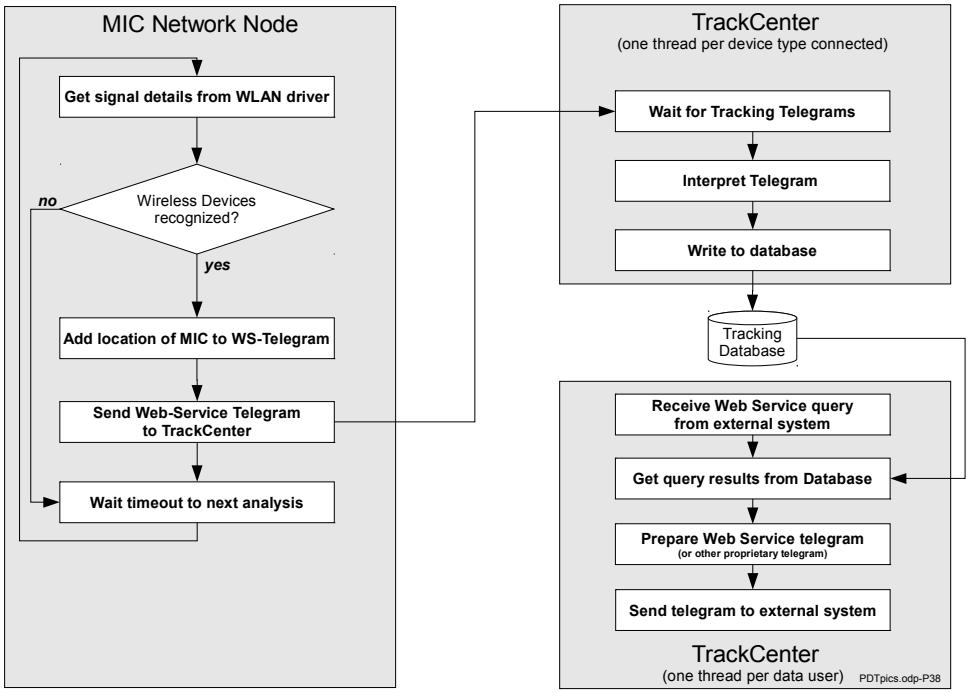


Figure 26: Data flow of tracking information

The related data flow is shown in figure 26. The information given in this figure is principally handled identical for tracking information other than WLAN signal based data acquired by the Network node. In these cases (like RFID readers) the location of the reader will be added instead of the MIC's own location. The telegram created for sending to the TrackCenter however remains identical.

The TrackCenter runs a separate thread for each device type connected at a time. Web Service based threads are waiting for WebService telegrams to be received on their individual server ports. After receiving a telegram, its integrity is checked by the regular XML schema validation procedures [23] [24]. After successful validation, the telegram is accepted and the content is stored in the database.

Requests to the TrackCenter are handled by different separate threads each representing one separate connector [14]. Via such connector, a query request is received and the results are acquired from the database before issued as a response to the sender via a related telegram. Preferably, these requests are handled via WebServices, too. However also proprietary connectors are implemented individually. The main external connector is the one used by the ViewCenter in order to display the locations of people and machines graphically.

4.1.6 PagerCenter Implementation

The PagerCenter is a platform to prepare, send and store text message communication to handheld devices, namely pagers and smartphones capable of running this particular message communication which has an important role for both the operational communication in a mine and for the safety support communications: As it does not require expensive phones as handheld devices, more people can be equipped with pager devices (chapter 3.3.2).

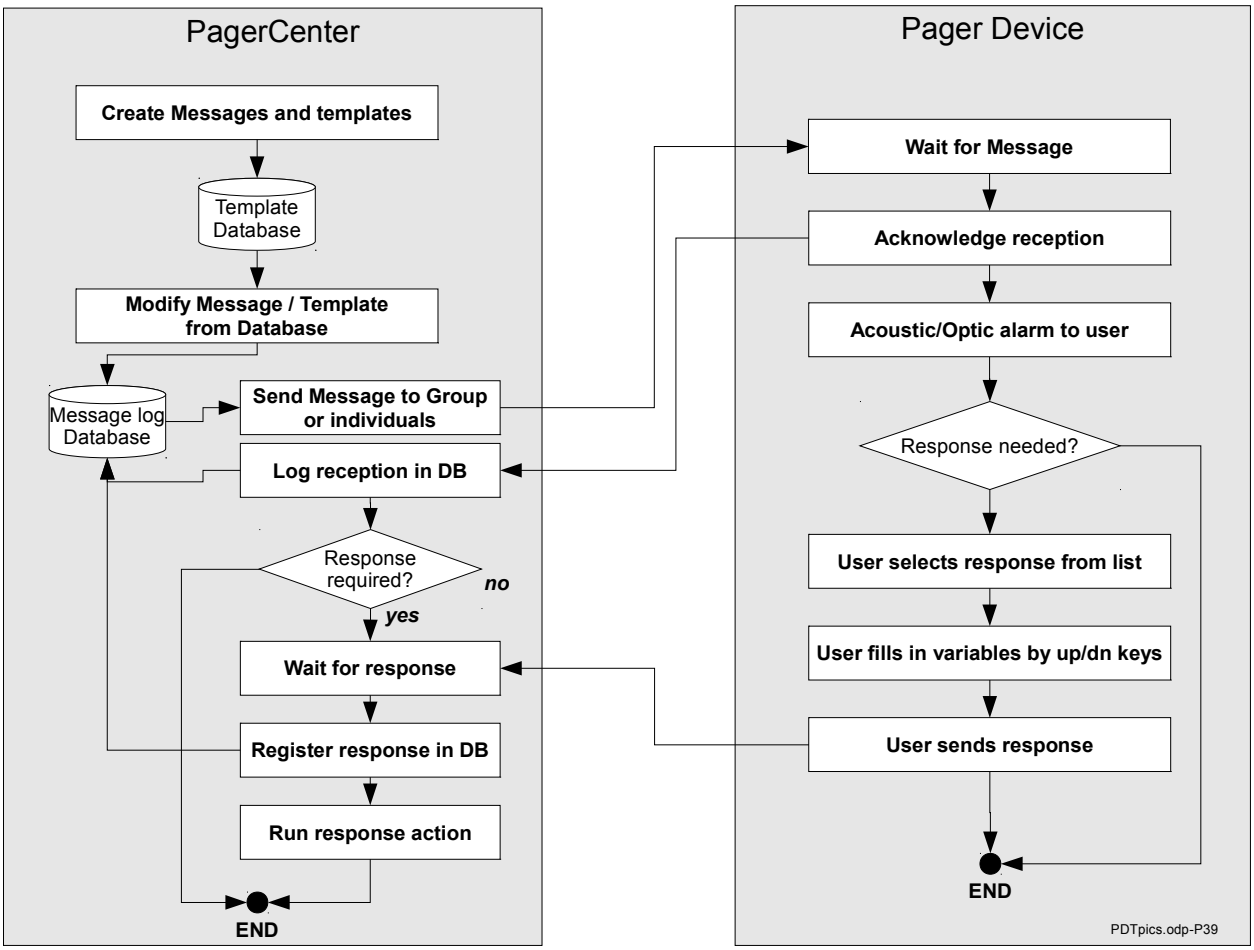


Figure 27: Interaction between PagerCenter and Pager device

Upon creation of a message, the user via the Web User Interface of the PagerCenter selects a message or a message template from a database (fig. 27). This message is then modified and stored in a Message Log database containing all messages processed together with their status and time of delivery as well as time of reading. The message exchange has to take into account that not all devices can be regarded online all time, so the PagerCenter's send function tries to send it continuously in short time intervals until the device can be reached [13]. When the message has been sent successfully, the device acknowledges it's physical reception, which also is stored in the Message Log database. The user on the mobile device is warned by optic and acoustic alarm [12].

The further processing on the pager device is dependent on the fact whether or not a response is expected. In case a response is expected, the message sent contains a list of responses which the user selects one from for returning to the PagerCenter. If needed, he can also modify some variables by pushing the arrow keys on the pager device. When ready, he sends the message back to the PagerCenter [12].

When the response arrives at the PagerCenter, the response is stored in the Message Log Database. If configured for this particular event in the Template database, a notification is sent to a list of recipients. This could in turn be a message to another person or group or an email.

4.1.7 VoIPCenter implementation

The VoIPCenter organizes all Voice-over-IP audio communication over the underground network. It consists of a standard ASTERISK PBX under a LINUX operating system [103][82].

The user interface for the VoIPCenter consists of a web application which can be started from a dispatcher workplace, whereas multiple dispatcher workplaces are possible to use. The dispatcher has the possibility to call single participants as well as entire groups. A special use of the conference functionality provides "*push-to-talk*" functions. This is a use of the VoIP system similar to the use of walkie-talkie radios where one person speaks after pushing the *talk* button and all participants on the channel (or in VoIP terms in the particular group) are able to hear.

For use with the Safety Support system in Emergency Mode, a scaled down version of the ASTERISK PBX is available on each MIC network node to run on the network node's OpenWRT LINUX in order to be started for local VoIP communication in case all connections to above ground are lost (see chapter 2.5.5).

4.1.8 ViewCenter implementation

The ViewCenter 3D mine visualization for location based display of status information from the underground mine (chapter 2.5.6) bases on a 3D engine and mining specific addons provided by Xgraphic Ingenieurgesellschaft, Aachen, Germany [55][54]. This software is used in a customized (re-branded) form under the name "*ViewCenter*" by MineTronics.

In these application, the ViewCenter is used only for visualization of tasks and status information acquired by other Center servers and also from third party systems in the mine. There are no application specific parts implemented in the ViewCenter, except of those directly

and exclusively related to the visualization of information.

For display of tracking and network status information, mainly interface software development is required to implement the Center server Web Services to be used by the ViewCenter to import all related information for visualization.

Precondition for each ViewCenter application is that the mine map is imported from 2D or 3D CAD data. This is in most cases a manual procedure as the CAD information not always completely matches reality and adjustments between real world and model nearly always have to be carried out.

4.1.9 SafeCenter implementation

The SafeCenter provides all data related to the underground safety related applications. In the sense of the Network based Safety Support application these functions are:

1. Storage of all static data which the network nodes need for performing their independent safety support functions
2. Transmission of all static safety data to the network nodes upon initial startup of the network node (or when the node is moved to another location) and upon change of data.
3. Acquisition and storage of all safety-related operational data from the mine (like Sensor data, environmental data etc. if not performed by a different server
4. After an emergency: Store all data collected from the MICs during the emergency
5. Transmission of all safety related information to the ViewCenter visualization for display on safety layers inside the mine model.

4.2 Functional Implementation - Overview

4.2.1 Safety Support Services

The Safety Support Services are software components running on the MIC network nodes, which handle all application level functionality of the Safety Support System during regular operation in Normal Mode as well as during Emergency Mode as described in the following chapters. These services, which are mostly running as a number of LINUX processes on the stationary and mobile equipment explained in the previous chapters, implement all local functionality such as [98]:

1. Determining the network topology as precondition for Emergency Mode detection and Emergency Mode services (chapter 4.3)
2. Emergency Mode detection (chapter 4.4.1)
3. Assignment and Launch of Central Network Services (chapter 4.4.2)
4. Interpretation of safety cases from sensor data and estimation of hazard locations from network and sensor data (chapter 4.5.1)
5. Guidance Application to guide people to a meeting place or exit (chapters 4.5.4f).
6. Tracking Application to detect whether people are left behind during self escape (chapter 4.5.4)

In addition, two services are needed which are not exclusively used in Emergency Mode:

1. The Topology application (chapter 4.3) is running permanently as it is also needed for determining the network layout and for switching redundant network links.
2. The Messaging application which issues text and alarm messages to the people in the network in proximity of the current MIC (see 3.3.2.) This application does not directly belong to the Safety Support Services so it's implementation is not described in detail in this document.

Programming of these services is performed in C/C++ following strict rules in terms of programming style and especially memory handling [6]. According to these rules, dynamic memory allocation is discouraged once a program has finished it's configuration phase. This rules assure a reliable long term operation of the embedded software generated.

4.2.2 High Level Working Sequence

The general working sequence of the Safety Support System is illustrated in figure 28. [98]. It consists of:

1. Startup and initializations (1.x in fig. 28, see chapter 4.2.3)
2. Normal (regular) operation with permanent Topology and status communication

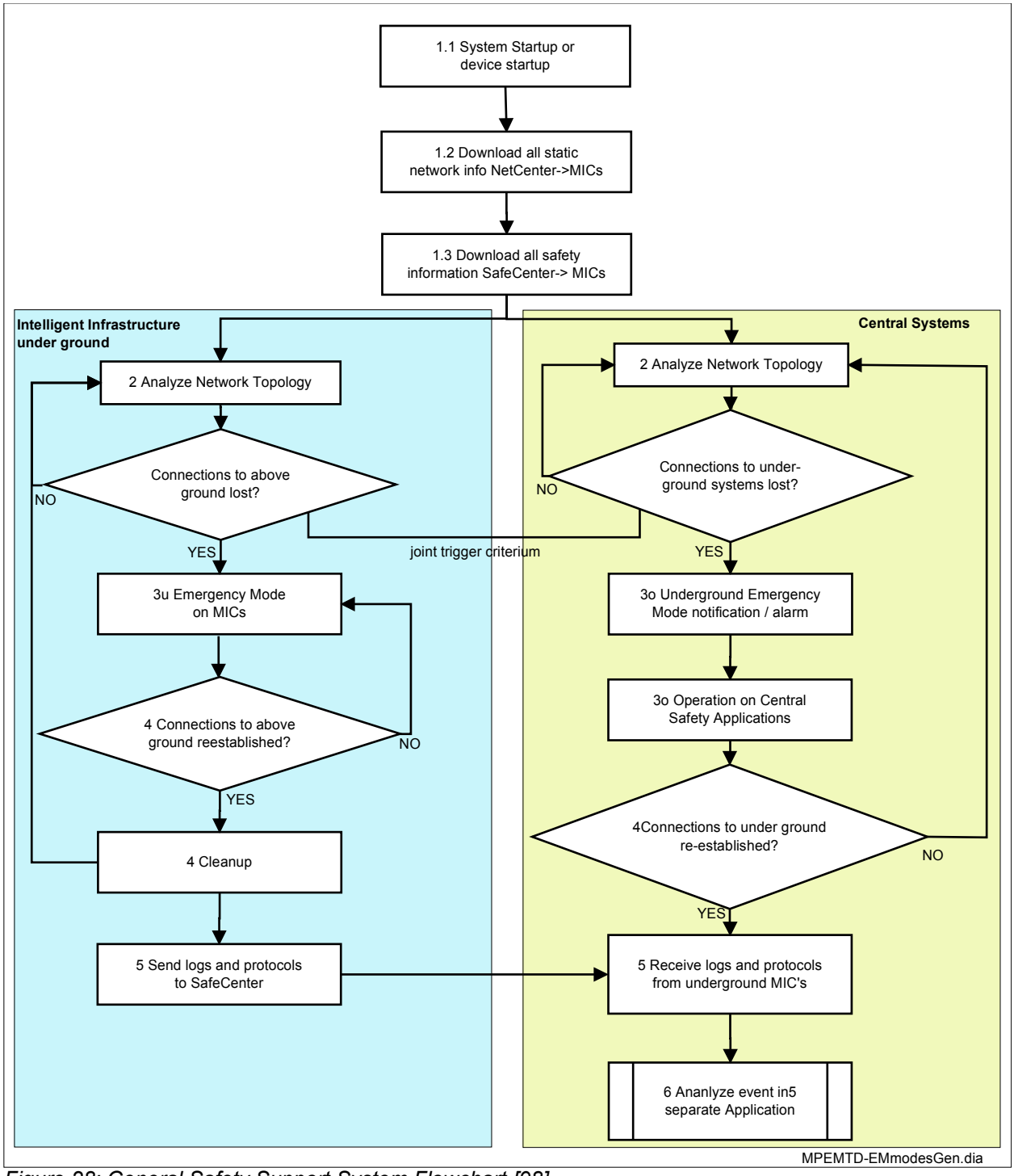


Figure 28: General Safety Support System Flowchart [98]

between underground and above ground systems (No. 2 in fig. 28, chapter 4.3)

3. Emergency detection and emergency mode procedures underground (No. 3u in fig. 28, chapter 4.5)
4. Emergency support services above ground (No. 3o in fig. 28, chapter 4.6)
5. Network recovery and cleanup of Emergency Mode (No. 4 in fig. 28, chapter 4.7)
6. Upload of all emergency mode data to SafeCenter server (not part of this project)
7. Offline analysis of the emergency event by special analysis software (not part of this project)

A general description of the sequence is shown in figure 29 together with important annotations.

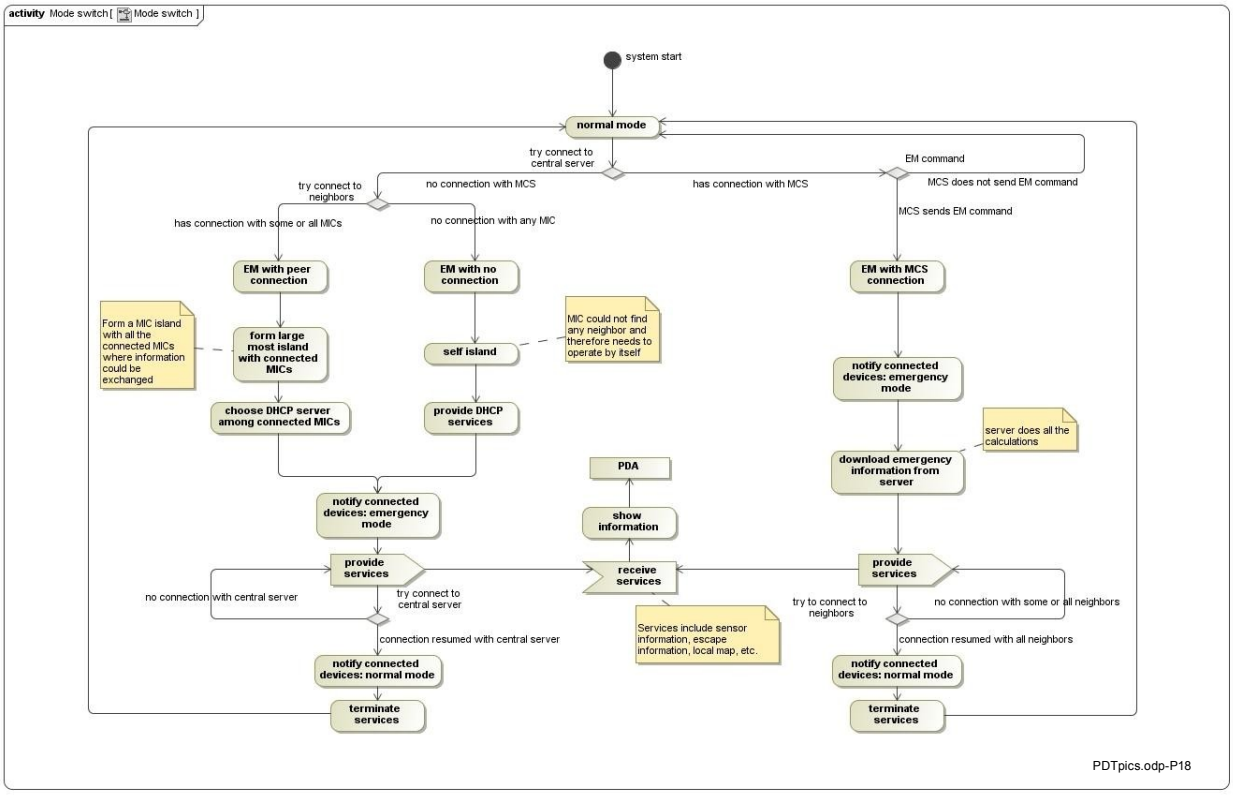


Figure 29: Illustration of the general working sequence

Emergency Mode always is triggered by connection loss between above ground and underground. After this detection, the underground network has to establish central network services first before providing the Emergency Mode application services .

Figure 30 shows a more detailed flowchart for the underground systems after initialization. The numbers in each step in figure 30 are later used for uniquely referencing the

steps, which are described in detail in the following chapters.

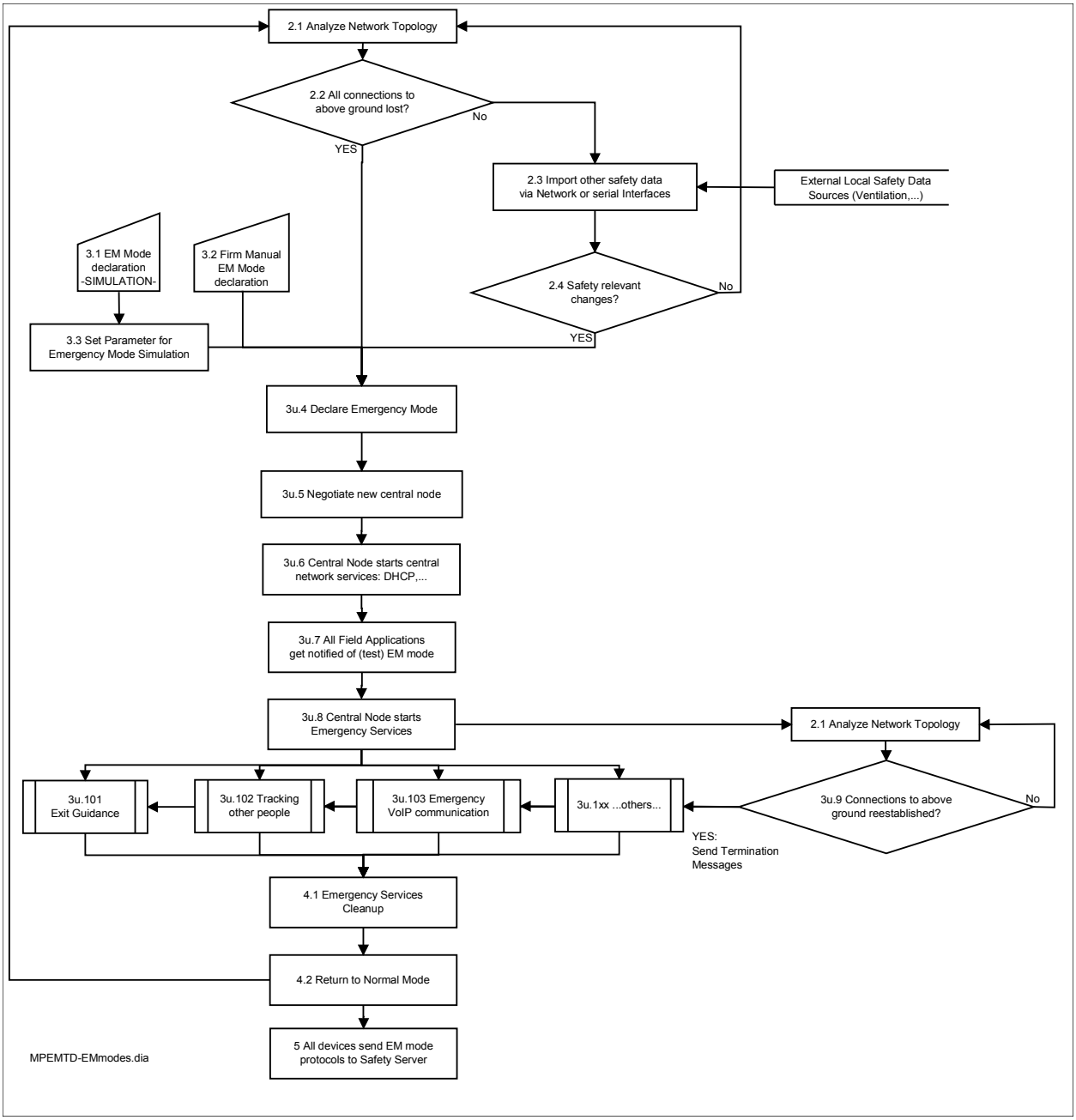


Figure 30: Overall system operation flow

4.2.3 Start up and initializations

At initial start up the above ground servers (NetCenter and SafeCenter) have to be started first. This is because otherwise the underground network nodes (*MICs*) will not "see" any above ground server in the network when they are initially started and the underground Emergency Mode has to be started without the MICs having got their basic working configurations.

Due to this fact, the underground MICs are configured to provide network services but no

Safety Support services until they have gathered all static information from the above ground systems.

When a MIC starts for the first time, it directly is able to run it's configured network functionality. However there are configurations necessary of where exactly the MIC is located in the mine etc. Therefore, it will fist show up on a list of unassigned nodes in the NetCenter. When assigning the required configurations, it will get it's geographic location and other data relevant for operation and safety support.

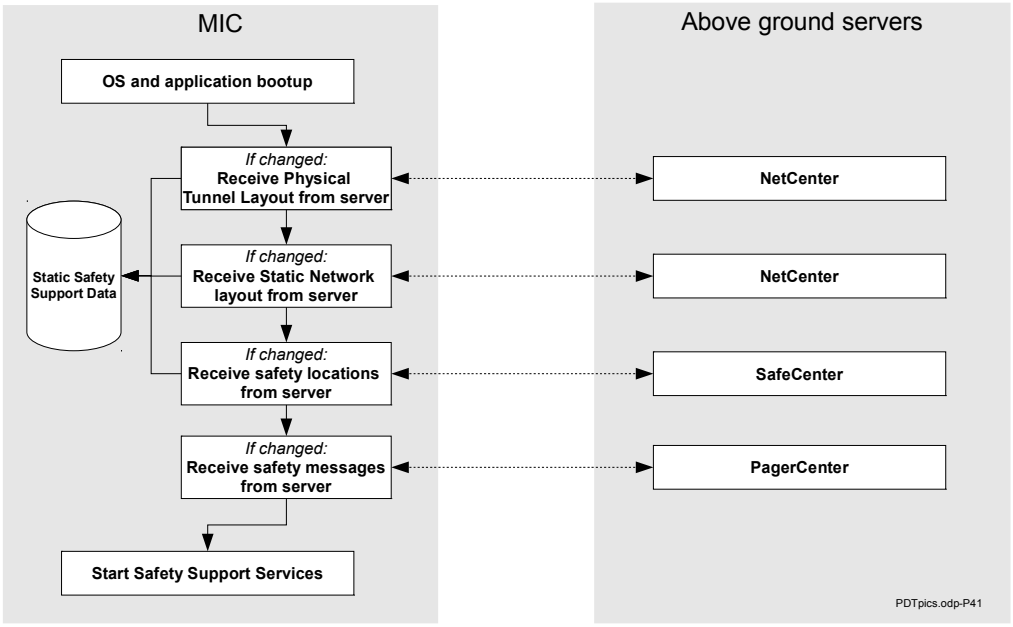


Figure 31: Network Node Startup Initializations

After these configurations have been made, all relevant static network information about the mine layout, the static network topology and related static safety information about e.g. the location of rescue shelters, fire fighting equipment, emergency exits etc. is downloaded from the central systems to the MICs (fig. 31 and chapter 2.1.1).

In a first implementation, each MIC thereby receives the entire static information about all the mine or at least about the whole area handled by the assigned above ground server. This may be not very efficient especially for very big mines, however it is a simple way to start with in order to be able to verify the system principles.

As soon as the static configurations are checked and updated by the routine described above, the MIC network node starts it's Safety Support Services.

4.2.4 Emergency Mode Coordination

As the Emergency mode automatically is triggered upon connection loss between the underground network and the above groua linked liet nd central systems, namely the *NetCenter*, the overall processing is split as soon as the Emergency Mode has been detected (chapter 4.3). In this connection the term "*Underground Network*" means that the underground network as a whole or a random part of it can be disconnected from the working rest of the network:

- The underground units now work in an isolated mode (chapters 4.4.2 and 4.5)
- The above ground central systems work in an isolated mode (chapter 4.6)

This split processing makes it important that the underground systems store all real time safety relevant data (like people tracking information) in an intermediate non volatile memory buffer. After contact to servers is re-established and the network returned to normal operation mode this data is sent to the above ground SafeCenter server for post event analysis, however this was not part of the ongoing project. For this purpose, the non volatile Flash memory is extended in the newest generation MIC network nodes. This safety relevant data consists of e.g. the availability of network nodes, link statuses, tracking information of people and machines, gas sensor data, availability of electricity etc.

Thus, in case of an emergency, the situation prior to the connection loss is available to both underground workers and the above ground rescue teams. Also the short term history can be of importance in the control center to assess the situation.

Now, during handling of the Emergency Mode, it is important to find the most efficient, safest and fasted way to evacuate and rescue people under ground. The availability of identical pre incident information underground and above ground together with clear and unequivocal handling instructions helps in such situations, even if most of the behavior underground is situation dependent and therefore very dynamic. However in practice every such situation to a high degree will be individual, the probability of the people underground do in this situation what the above ground rescuers assume basing on their pre incident information will become much higher than without having access to any pre incident information at all.

At least the rescuers above ground may analyze the situation and limit the possible actions e.g. to two possibilities where e.g. the people underground are located after the network guided them all to a central location. Consequently, the rescuers will handle these two possibilities with their highest priority.

This emergency mode rescue handling however is not part of this implementation. This may be subject to more mining related coming research work.

Another coordination issue however is important for the underground Emergency Mode handling in the communication system. This is the procedure of testing and training the Emergency Mode both underground and above ground together with the prevention of unintentional triggering of the Emergency Mode e.g. during connection losses caused by maintenance of the network system.

For training and testing purpose, the activation of the Emergency Mode can be simulated (Step 3.1) without affecting underground production. In this case, the triggering of a real Emergency Mode can be masked out (inhibited) in order to allow network maintenance etc (Step 3.2). Masking out always has to be performed with an given timeout in order to allow a fallback to regular operation after a given time to prevent from people "forgetting" to reset the inhibiting configuration. This is implemented by special virtual LANs ("VLANs") which are used in order to maintain the full network functionality and for not to impact production during the test or training. The "*Connection Loss*" situation is then simply triggered by configuring related switches to stop forwarding the related VLAN packets.

When due to maintenance, a network section underground has to be physically disconnected from the mine backbone network, the MICs in this section normally would trigger the Emergency Mode.

In this case, all related MICs can be configured to masking out the Emergency declaration basing on a previous configuration. This Emergency Mode inhibiting may be configured for a start time and a duration either via the NetCenter or individually via the MICs web interface. After this duration or after reconnect before that timeout, the MICs automatically return to regular operation mode. The configuration of the duration or end time is essential to prevent from intended or unintended suppression of the Safety Support functions. Also such configurations only have to be allowed by a very limited number of persons only after authentication.

4.3 Network Topology Determination

This chapter covers the function in item No. 2.1 in accordance to figure 30 "*Analyze network topology*", represented by the Topology Application software running on each MIC network node. To simplify implementation and internal communication this also combines a number of other functions for the Safety Support system and is therefore the central application to handle this distributed functionality:

1. Determine the network topology so every single network node has a full picture of the network's current logical layout which he is able to compare with the hardware layout as downloaded from the NetCenter (see 4.1.4 - Item 2 in fig. 28)
2. Detect communication loss to the NetCenter
3. Determine the Center Node of an isolated network (part of item 3u in fig. 28) as described in chapter 4.4

The Topology Application runs on every single MIC. It permanently analyzes the status of all network devices and all network links between the devices in order to detect sudden malfunctions, which in turn may be caused by an underground emergency.

An identical Topology Application, however with a different configuration, runs on the NetCenter so during Normal Operation Mode, both the central systems and the network nodes are working on a completely identical network status image.

The information acquired locally (4.3.3) or remotely for the full network using the protocol of the *Topology Application* (4.3.4) is stored in each MIC which thereby gets an overview of the momentary status of the network (4.3.2). In order to be able to compare this status to the situation how it should be when all devices are functional, the latter basic information about the "regular" network layout is downloaded upon system startup (See 4.2.3 and step 1.2 in figure 28). This storage is performed separately and not part of the Topology Application.

The link between the momentary situation and the static network information is the unique identification of the MIC's. Their geographic location in the mine links the network node to particular places in the mine and enables the calculation of escape routes.

By this set of information, each node is able to independently evaluate the entire network situation by comparing the momentary situation to the predefined situation. The delta between

those will be the relevant information for the following Emergency Mode trigger decision.

As this delta contains dropped links versus links which should be used, the fact that a link has dropped may also be interpreted as a potential Emergency location.

This makes the Topology Application conform the central part in detecting an emergency and in providing the network functions under ground in Emergency Mode.

4.3.1 Components and Design

The Topology Application consists of two processes (fig. 32):

1. The main application process
2. The network detection process for network neighborhood evaluation (4.3.3)

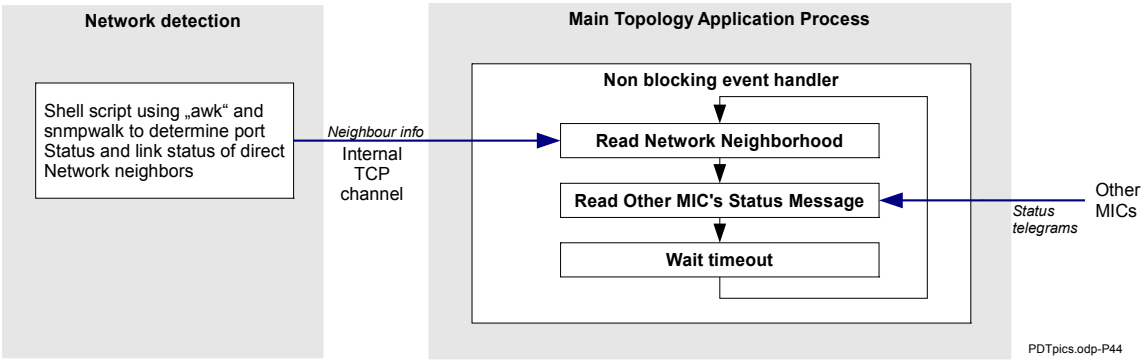


Figure 32: Topology Application Processes

The design goals of the Topology Application were to create a simple application to achieve a highest possible program stability and reliability using a smallest possible amount of resources in order to be run on low power hardware (chapter 3.2.3.3). This was leading to a plain C++ Application not using any programming convenience tools, databases etc. The class diagram of the application which the following chapters refer to is shown in the Appendix.

4.3.2 Internal Data Storage

Central part of the Main Topology Application Processs is the storage of the current network layout in the `NetNodeList` class (see class diagram in the appendix). It is initialized by the `NetNodeAllocator`, which preemptively physically allocates memory for a number of configured (“`max_num_of_nodes`”) network nodes. This allocation is intentionally not performed dynamically within the operation loop in accordance with the company's coding rules [6]. The allocation is performed during the initialization phase in order to prevent from potential

memory handling and re-allocation problems after a long system uptime and software reliability problems resulting from that [8].

In this sense, one object in the `NetNodeList` is allocated per MIC System (see 3.2.3.7) regardless of the number of physical switches contained in this system. The `NetNodeList` aggregates a `NetNodeAllocator` and calls its `allocate` method in case of new node is needed [8].

Each allocated object is then filled with the detail functional information from each of the `NetNode`s. This results in two linked lists [137] inside the data storage: One linked list containing the working data and another list with empty elements or such deleted from the list administering the free space available for new objects in the list [137], making it a linked list with free space management, thus preventing from dynamic physical memory handling.

The list is created in the order of the `unique` element, which contains the unique serial number of the MICs and acts at the same time as key [8].

The linked list setup provides a safe and very fast to process linear dynamic data structure, which however does not yet match the node-vector matrix relations between the NetNodes representing their connections among each other. This is handled by the content inside the `NetNode` elements in the linked list: Each `NetNode` element contains a list of max. eight neighbors (`neigh` element) which is stored with it's hardware address as identifier. By these links an indirect neighboring matrix is created without having to allocate the space for a physical matrix [8].

The `NetNodeList` has search functions by the `unique` identifier and hardware MAC address. Finding a node would result in the following source code statement [8]:

```
NetNode* find(const Unique& -unique);
```

This statement returns a pointer to a node, which belongs the unique id. If the node is not available it generates one by the allocator. It can return NULL only in case of an out-of-memory exception[8]!

The statement

```
NetNode* find(const HwAddr& hwaddr);
```

returns a node which has a network interface with the hardware MAC address `hwaddr`, otherwise NULL [8]. It shall be noted that several hardware MAC addresses can point to the

same node, as multiple switch modules are used inside a single MIC system (see 3.2.3.7).

The data about each network node contained in the linked list includes the following:

- HW MAC Addresses
- IP V4 / V6 addresses
- Geographic location
- Number of network interfaces available
- Status of each network interface:
  - Active (link used)
  - link available but not used (blocked by RSTP)
  - Inactive (no connection)
- Age of data stored (time last update etc)

Information about the neighbors of the specific node

4.3.3 Network Status Detection

The neighbor info acquired locally is used to update the local NetNode elements about the neighbors found and to create the Status Telegram which is sent to all other nodes in the network.

The acquisition of the network neighbor status is performed by an external awk [2] script, which communicates via an internal TCP channel with the `RingUpdater` class of the Main Topology Application.

The awk script contains an *snmpwalk* [127] command to gather information about the identification of the neighboring nodes and the status of the network links to those nodes (fig. 33). *Snmpwalk* is a *Simple Network Management Protocol* (*SNMP*) [152] application that uses the SNMP GETNEXT requests to query a network entity for a tree of information [127].

This makes all information from each queried device available to the issuing MIC, which is available from this unit via SNMP.

First, the script acquires the port status using the following command:

```
snmpwalk -Oenv -v 1 -c private host_ip 1.3.6.1.2.1.2.2.1.8
```

For each active port, the script then retrieves the hardwarea addresses of the neighbors:

```
snmpwalk -Oenv -v 1 -c private host_ip 1.3.6.1.2.1.17.2.15.0.8
```

The results come in form of a SNMP object tree, which is a text file parsed by the awk script of the Network Status Detection process in order to filter out the data needed for the Main Topology Application Process. The results are transmitted via the internal TCP channel to the `RingUpdater` class in the Main Topology Application.

The `RingUpdater` class updates the status of the network node the application is running on (`mynode`) in the `NetNodeList.` This data then is also used for the creation of the Status Telegram according to the following chapter to be sent to all other nodes in the network.

4.3.4 Protocol and Message Exchange

4.3.4.1 Communication Layer

The topology application uses a multicast or broadcast routine to distribute the Status Telegram over the regular network to all other MICs and the NetCenter in the system. For this transmission the UDP protocol [153] is used without having to establish dedicated transmission channels before the messages are sent. This however also means that no dedicated acknowledge is being issued by the receivers to the transmitting node, which is not required as only hard wired connections are used to transmit these messages, which can be regarded highly available and the fact that the messages are repeatedly communicated quickly compensates possible errors .

On the other side, the broadcasted UDP protocol provides a very resource efficient way of communication which is to be regarded very important as this administrative communication shares the medium with all application level communication routed through the switches.

The communication is implemented by using the `RawSocket` class (see class diagram in the Appendix). In this connection it has to be emphasized that this `RawSocket` class may not be misinterpreted as a real raw socket in the sense of the TCP/IP protocol family socket programming interface [154]! `RawSocket` here rather represents a regular application level class name [8]. In this class the member functions important for sending and receiving the Status Telegrams are:

```
ssize_t send(const void* ptr, size_t len);
```

This function transmits `len` amount of bytes from the buffer pointed to by `ptr`. It returns the number of bytes sent or -1 in case of error [8].

```
ssize_t RawSocket::recv(void* ptr, size_t len);
```

Receives maximum `len` amount of bytes into the buffer pointed by `ptr`. Returns the number of bytes received or -1 in case of error [8].

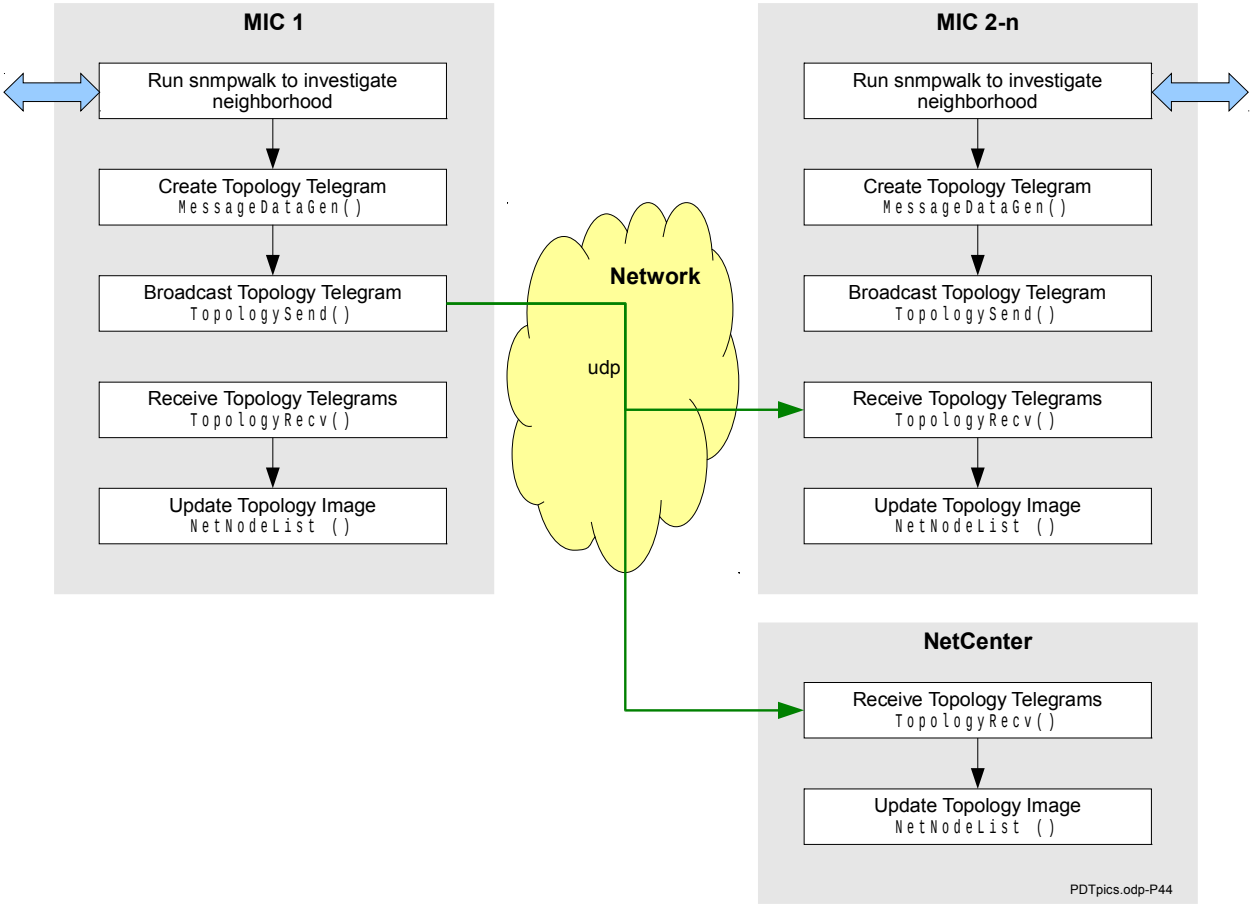


Figure 33: Topology Application Communication Flow

4.3.4.2 Message Content

The Topology Application protocol is defined by the `Message` struct (see figure 34). The `payload` element in `Message::Data` contains a series of Type-Length-Value based elements [153]. Each TLV has a type and a length field defined in the TLV struct in identical way for all tags to simplify interpretation of the telegram. All items in the TLV payload are in network byte order.

The structure of the protocol thereby can be flexibly extended if needed. The message content including the payload tags generated in the class MessageDataGen tags are:

`TLV:Ether`	Hardware Address, entry generated through `addHwAddr()`
`TLV::IPv4`	IP V4 Address, entry generated through `addIP4()`

`TLV::IPv6`	IP V6 Address, entry generated through `addIP6()`
`TLV::Coord`	Coordinate of the node, taken from the node's configuration, as X, Y, Z coordinates
`TLV::Neigh`	Address of the neighbor nodes

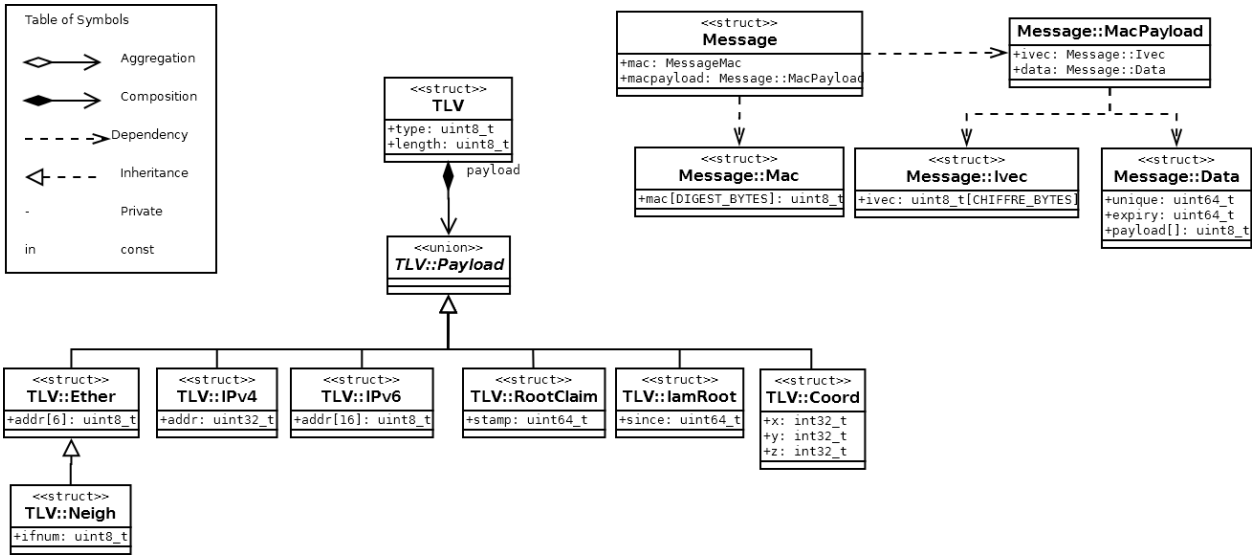


Figure 34: Message classes (Extracted from class diagram in Appendix)

This results in a flexible length of the message, which is determined by the function `getLen()` in order to assure the message is sent with the right length information.

In addition to the content explained above some additional information is needed to secure the communication:

4.3.4.3 Securing and sending the Topology Telegram

All messages are encrypted and authenticated to fulfill up-to-date network security goals, even if this may not be regarded essential in an underground mining environment [123].

Encryption is performed during `TopologySend()` function through calls to the `Chiffre` class using the encryption vector in `ivec.` The member function responsible for encryption is the `Chiffre::encrypt()` function which encryts the message data in place. It's `data_len` parameter describes the length of the messages data only which is built up the series of TLVs. The return value is the length of the encrypted message data, which could be longer due to some zero padding added [8].

After encryption the authentication is performed within the `Digest` class within the `digest()` member function which generates the authentication vector for the message data.

Important for this function is the fact that the message length used for authentication is the length of the message data plus the length of the encryption vector.

4.3.4.4 Receiving the Topology Telegram

After reception of a message by the Communication layer (4.3.4.1) and through the `TopologyRecv` class, the verification is performed by the `Digest::verify()` function. If the verification is successful, the message is decrypted in `Chiffre::decrypt()` after which the message is parsed and interpreted in order to be finally stored in the `NetNodeList`[8].

4.3.5 Helper functions and data structures

Some helper functions and structures are needed for the main functions to be able to work. These are mainly functions to read processing relevant information like:

readNetstatNode	determining the IP address of the own device
readMyCoord	read the location from the appropriate configuration file
readUniqe	retrieve the own unique key

The unique key is representing an unique id for each node. It is generated in the same way as an ssh key and is stored in a permanent place like in the EEPROM area of the MIC's Baseboard ATMEL microcontroller (3.2.3.2) [8].

The `coord` structure represents a geographic location in the mine with x, y and z coordinates in the mine's coordinate system. In later implementations this should be replaced by an IREDES standard compatible [70] coordination data format.

4.3.6 Generate XML output

A special function normally only activated in the NetCenter version of the Topology Application running above ground is the generation of XML output from the NetNodeList which makes the entire NetNodeList and the relations between the nodes available to third party computer systems. This is performed by the XmlGenerator class basing on a XML schema (see Appendix).

The resulting XML file output is used directly by external graphical programs (like NetView running on the NetCenter server) to show a graphic representation of the underground

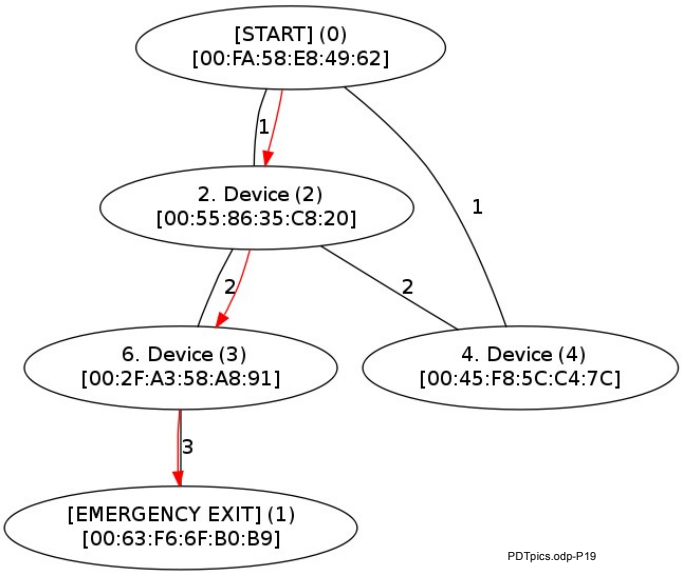


Figure 35: Simple graphic output generated from XML file

network setup similar to the simplified output in fig. 35, which also can be used in similar way to generate simple graphical output to guide people in emergencies. For this reason the related functions are also available on the underground MICs.

4.4 Emergency Mode Detection and Startup

4.4.1 Emergency Mode Detection

Elementary part of the Safety Support Services on the MIC is to handle the detection of an Emergency Mode. This is performed by the Topology Application (4.3) which nevertheless sends status messages in regular intervals. The Emergency Mode detection thereby is part of this protocol exchange and is implemented as follows:

In the message `Payload` data structure the `TLV::IamRoot` tag is always set by a node if the node itself carries out the root (Center Node) function. During Normal Operation, the Center Node is represented by the NetCenter server above ground (see 2.5 and 4.1.4). The NetCenter is not the physical center of the network, but under regular operation it provides all the central services making it logically acting as Center Node.

As the NetCenter server runs the Topology Application in identical form as the underground MIC network nodes, it is configured to set the `IamRoot` tag in all the status messages it sends to the network nodes inside the underground network.

When the (redundant) network contact to above ground central systems and thereby also to the NetCenter server is lost, the underground network nodes will not receive the "`IamRoot`" marked Topology Telegram from the NetCenter server any longer. If this is persistent for more than a configurable amount of time, the Emergency mode negotiation is started automatically.

This routine works in any situation when the contact to the current root node is lost, regardless whether this is the NetCenter server or when the contact to a Center Node in an already disconnected network running in Emergency Mode is lost: In such case, the network simply splits up into two separate.

Also this procedure makes the Normal Operation mode continue seamlessly without any interruption when only a part of the network gets cut from a connection to the NetCenter.

4.4.2 Starting Emergency Mode underground

Even if this chapter only covers the Emergency mode as such, the runtime working sequence of the entire system is shown in figure 30 in order to be able to illustrate the entire sequence. Note that this chapter only covers the items indexed by "*3u.*".

After the system initially starts and after bootup and configuration of every device (chapter 4.2.3), each individual device starts analyzing it's network environment (Step 2.1 in figure 30) as described in chapter 4.3). In this step, the "*Topology Application*" in each network node determines the status of the other network devices in the environment together with all links between those network devices by creation of a full network status model. The lack of an "`IamRoot`" information in this communication (details see chapter 4.3) determines, whether a link to the above ground servers (namely the NetCenter) still is active.

During this time, also other safety relevant data available in the underground network is analyzed, like burning gases (CO) or potentially explosive atmosphere (e.g. CH4, Step 2.3 in figure 30). As long as all information relevant for triggering safety related actions is within preconfigured margins, no action will be performed.

If the Topology Application shows a failure of the connection to the above ground servers by lack of the "`IamRoot`" flag coming from the NetCenter, the devices start Emergency Mode negotiation (Step 3u.4 in figure 30). This will be the case after a full connection loss occurs and is unconditional as long as no parameters are set to prevent triggering Emergency Mode e.g. due to maintenance.

As a consequence of the lost connections to above ground all the disconnected (part of) the underground network also looses all central network services like the IP address assignment via DHCP, SIP services etc. For such central services, one single network node has to be assigned automatically among the nodes in the network in order to take over this "*master*" or "*Center Node*" functionality. This node then also has to set the "`IamRoot`" flag in the Topology Telegram again in order to continue services.

This new master node ideally is located far from a potential danger zone in the logical "*Center*" of the active network. The network center is defined as the network node with the most equal number of network connections ("*hops*") to any End Node in the network, whereas an "*End Node*" being defined as a node with only one single physical connection to the network (Nodes A, B, C and D in figure 30).

As each MIC holds a real time status image of the network setup (see 4.3), each node is able to determine it's position and the position of all other nodes inside the network, so the determination can be performed by every single MIC in the network in order to determine whether or not he has to take over as the new Center Node.

A precondition for applying any algorithm to find the center node is to define that logically inactive standby connections which are physically available but not used at the time of calculation are counted as available connections, because they any time can be made available via the *RSTP* protocol [60] as standby links in case of a failure of another link. The reason for this definition is mainly to prevent from too many recalculations of the Center Node once the Emergency Mode is started as it can be anticipated that the network structure also may change under such unstable external circumstances.

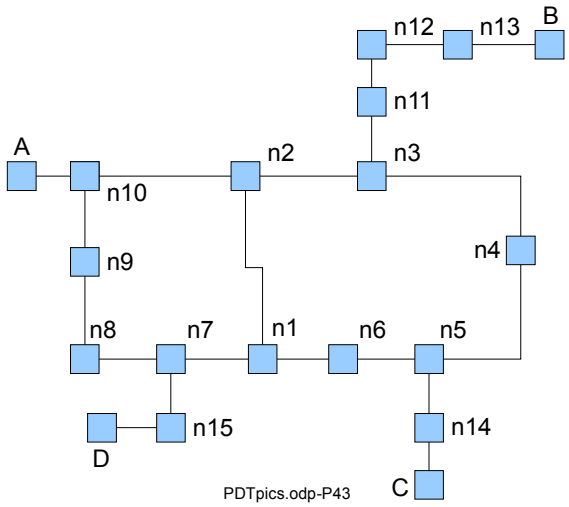


Figure 36: Sample Network Setup after disconnection from central systems

From these preconditions the Dijkstra algorithm [30] has been determined applicable to calculate the shortest path between any node and any end point in the network. This algorithm however originally is intended to calculate the shortest path between two nodes [30]. In case of this problem however the algorithm has to be applied to find the equally shortest path to all end points of the network, which is performed in accordance to the following procedure:

From the network Topology image inside the linked lists (4.3.2), every single MIC individually runs the Dijkstra algorithm to determine the shortest path of all nodes inside the network to all endpoints of the network. From this calculation every single node creates a similar matrix containing the number of hops from each node to each endpoint. A sample matrix is given in table 9 basing on the network example shown in figure 36.

According to the definition above, the center node is the node with an equally long route to all endpoints of the network, meaning the most equal number of hops to all endpoints. Therefore, for each node, the standard deviation over the number of hops to each endpoint is calculated. A calculation table for the example network in figure 36 is given in table 1.

	A	B	C	D	Avg	Std.Dev
n1	3	6	4	3	4	1,41
n2	2	5	5	4	4	1,41
n3	**3**	**4**	**4**	**5**	**4**	**0,82**
n4	4	5	3	6	4,5	1,29
n5	5	6	2	5	4,5	1,73
n6	4	6	3	4	4,25	1,26
n7	4	7	5	2	4,5	2,08
n8	3	8	6	3	5	2,45
n9	2	7	7	4	5	2,45
n10	1	6	6	5	4,5	2,38
n11	4	3	5	6	4,5	1,29
n12	5	2	6	7	5	2,16
n13	6	1	7	8	5,5	3,11
n14	6	7	1	6	5	2,71
n15	5	8	6	1	5	2,94
A	0	7	7	6	5	3,37
B	7	0	8	9	6	4,08
C	7	8	0	7	5,5	3,70
D	6	9	7	0	5,5	3,87

Table 9: Calculation Matrix for Center Node assignment for example in figure 36

The table shows all multi ended network nodes (*n1-n15*) and also all End Nodes (*A, B, C, D*) and the number of hops to all End Nodes. It also shows the arithmetic average and the standard deviation to determine how equal the number of hops is from the current node to all End Nodes.

As all nodes will perform an identical calculation, all will come up with an identical result in this case determining Node *n3* as the node with the lowest standard deviation. Consequently, node *n3* calls himself the new Center Node which continues processing in accordance to the left column in figure 37.

After this is calculated and after a node determines himself as being the new Center Node, he checks whether there is another node with an identical evaluation result available. If this is the case, the node with the lower `unique` field in the `Node` data (lower serial number) wins [8].

This node issues it's Topology Status telegram (4.3.4) to all nodes declaring himself the new Center Node by setting the "`IamRoot`" tag in the messages `Payload` structure (see 4.3.4.2). This message is received by all other nodes thereby disabling those to call themselves the Center Node (right column in figure 37). For safety reasons there is an additional timeout of 10 seconds in order to check whether or not another node called out himself as CenterNode. In this case also the lower serial number in the `unique` field is decisive to solve the conflict. This conflict only could origin from the fact that those nodes calculated their CenterNode assignment basing on slightly different Topology Data which may be the case in dynamic situations with quickly changing network structures, what in turn leads to the conclusion that when problems

occur in assignment in future versions the network matrix has to be frozen before all nodes start calculating the new Center Node.

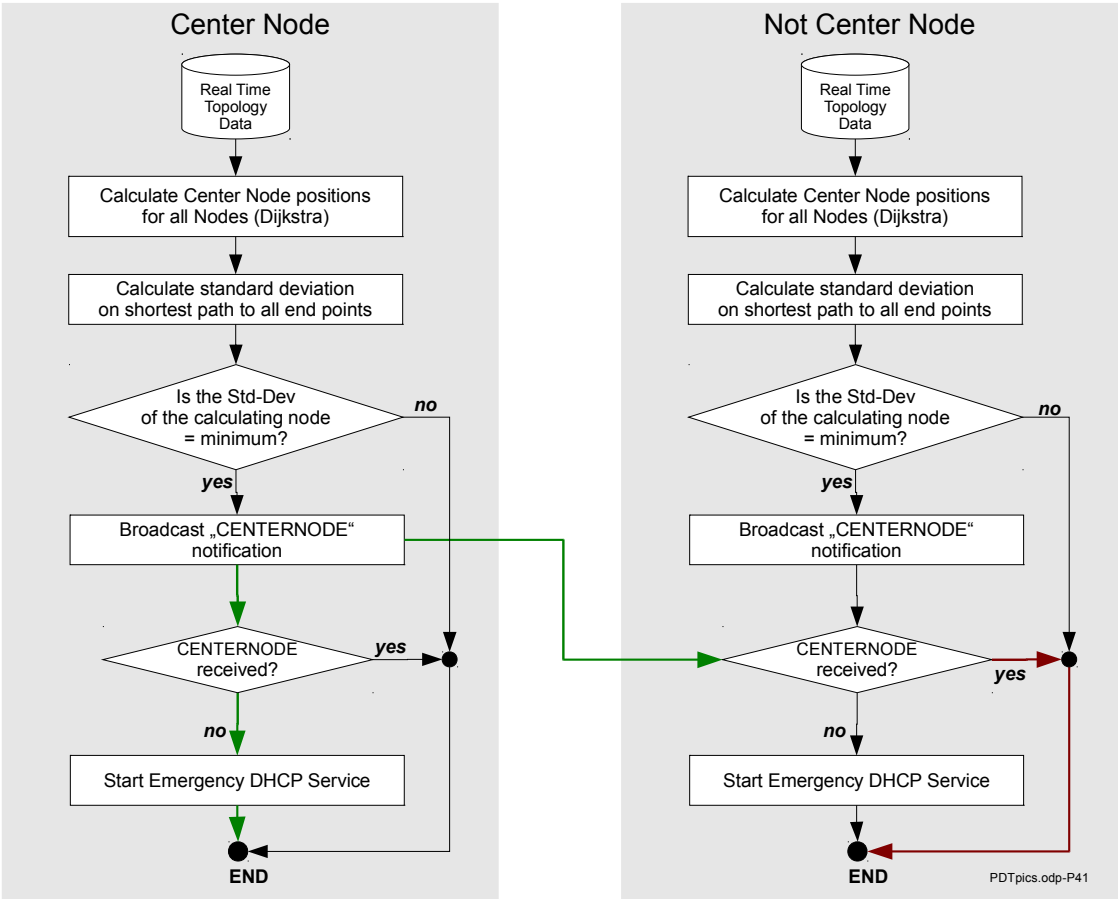


Figure 37: Center Node calculation

After the waiting time expired, the new Center Node starts the Emergency Mode DHCP service. Additional services like SIP for Voice-over-IP audio communication (chapter 4.5.3) or the Network Time Protocol (NTP) for time synchronization are also started on the Center Node. Alternatively it may be configured that the Center Node starts theses services on neighbor nodes. After this step, the network infrastructure is functional again.

Now, the Field Applications and especially the personal devices of the miners have to be notified of the situation. This notification includes an information whether the Emergency Mode is a simulated test or training or whether it is a real event (Step 3u.7 in figure 30).

Then, the newly defined Center Node initiates the start up of applications required for handling the Emergency Mode and supporting the people under ground (Step 3u.8 in figure 30 with sample applications shown as steps 3u.101-3u.1xx). These applications also may run on the

Center node itself as well as on neighbor nodes which the Center node triggered to start particular applications. For these procedures it is important that all applications and services are installed on every single node in order to allow full functionality in a network which, due to the emergency case, may be of completely random layout.

During all Emergency Mode, the Topology Application (4.3.4) keeps running on every node even during the Emergency State. If the Topology Application now determines, that that the connection to above ground is re-established by the NetCenter starting to send "`IamRoot`" tags again (step 3u.9), the Emergency Mode is canceled and regular service resumed (Step 4.1 in figure 30, see 4.7).

4.4.3 Dynamic IP address assignment

Nearly all underground clients are designed to use the Dynamic Host Configuration Protocol (DHCP) [165] for IP address assignment. When during Emergency Mode the underground clients need a new DHCP lease or if a device is reconnecting to the network, the DHCP address will be assigned by the Emergency Mode DHCP server on the Center Node.

The most important criteria for IP address assignment is that this process should be so convenient and invisible to the user as possible during assignment of a (new) IP address in Emergency Mode and also after returning to Normal Operation Mode.

An optimal solution would be to implement the regular DHCP failover peer routine, which requires a secondary DHCP server which carries on the DHCP service in case the primary DHCP server fails and is not reachable any longer [165][153][80]. However, in the application of the Emergency Mode it never can be predicted which alternate DHCP server will be available as such failover cannot be predicted to be a particular device. Experiments with failover solutions showed that a more extensive research to find a reliable solution is required (see chapter 5.7).

Therefore it was decided for the first implementation to run a simple solution which consists of the following procedure:

All devices in the underground network including the NetCenter run in one and the same IP subnet, which is an identical subnet in Normal Operation Mode and in Emergency Mode.

The primary DCHP server running on the NetCenter is configured to assign IP addresses only in a part of this subnet.

On each MIC network node, the Emergency DHCP server is installed in a configuration

which – upon activation of the DHCP server on a MIC network node – only assigns IP addresses in the other part of the subnet where the NetCenter does not assign any IP addresses.

One problem however cannot be prevented in this configuration which is occurring when two underground islands each operating in an isolated Emergency Mode are connected. In this case, both MIC based DHCP servers have assigned leases from the Emergency IP address range which most probably will lead to IP address conflicts in the network.

For this reason all DHCP servers are configured to assign short expiry times of the DHCP leases, which typically are in between 5 and 10 minutes so that it can be anticipated that after this time the network always will be free of IP address conflicts after such event.

An alternative however would be to run the entire system on fixed IP addresses which however seems unpractical due to the high dynamic of the use of mobile devices and the administration effort related to it.

4.5 Emergency Mode Applications and Organization

An *Emergency Application* is a software application running on mobile network devices used underground or running on stationary devices installed throughout the underground network. Emergency Applications have the following purposes:

1. Emergency Location detection support
2. Support miners underground to assess the Emergency situation
3. Help the miners to get together and meet each other in the isolated area
4. Help the miners to find emergency equipment (fire fighters, first aid,...)
5. Help the miners to evacuate or to reach safe areas (shelters etc) by a controlled guidance
6. Assure that nobody left behind during walk to a meeting point or to an exit

4.5.1 Emergency Location detection Support

A safety critical situation can also develop while the network is still available. Also such situations are supported by the system: This may be the case when safety relevant data like environmental sensors concludes a safety critical situation. If during this time a network link or an active device stalls, the underground network is interpreting these facts to trigger safety actions. This computation is performed by individual application programs directly on the MIC computers in proximity of the safety related sensors in the field. This is explained in detail by the following example:

It may be anticipated that e.g. CH4 sensors detecting potentially explosive atmosphere or CO sensors detecting burning gases show values (blue line in fig 30) raising up to a warning or even alarm level (represented by the orange area in fig. 30).

In order to detect such situations, the MICs read all network available sensor information assigned to them and store an event history of network and safety related events from sensor systems in a ring buffer. This processing is highly dependent on the safety sensor systems used and whether or not the communication is carried out via network or via conventional RS485 links. For such systems, a serial connection is available for the MICs so serial systems can be connected, also in parallel to the existing serial communication. The MIC then stores the incoming sensor in a conventional ring buffer data structure again set up as circular linked lists

with the time of acquisition as main order criteria, thus conforming time series data to be stored.

The set values for triggering an alarm are part of the Safety Data overlay to the mine map which is acquired from the central systems upon system startup enabling the MICs to compare the warning or alarm thresholds to the real time values.

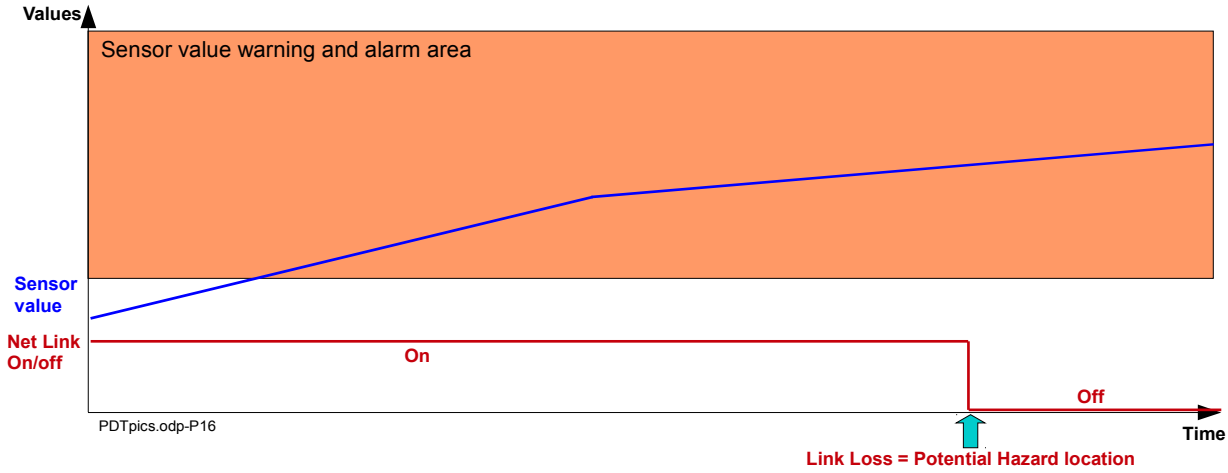


Figure 38: Safety Sensor values and Hazard Localization via Network Link Status

While an environmental sensor data being above an alarm threshold, a network link or a MIC in the area stalls and is not available any longer e.g. due to a fire. This network status change and it's location is determined by a "*Topology Application*" running on each MIC (see chapter 4.3).

After this combination is performed, the MIC informs the SafeCenter about this and triggers a related alarm in the mine control room. At the same time, also people in proximity are automatically informed about the sensor values and the location of the communication loss as this is a potential hazard area.

In this situation, the MIC's do not start an independent Emergency Mode as long as a logic connection to above ground is established.

If after such event however the connection to above ground is lost (as the disconnected link was the last one available), the probability is very high that the tunnel where the connection loss occurred is not passable for evacuation which finally is taken into account by the guidance process of the Safety Support Services (chapter 4.5.4f).

4.5.2 Emergency Situation Assessment

Potentially isolated miners underground in the beginning of an emergency case have absolutely the same information about the situation as the rescue people above ground as this is the latest information exchanged before the emergency occurred. Over time, the information available to the people underground however will deviate from the information of the rescue teams as the situation changes, the people underground will start to perform self-escape actions and the rescuers will start to localize and access the underground people from the outside.

Therefore, an assessment of the situation first bases on the last information available prior to the event occurred. This assures that identical conclusions will be drawn above and underground. An important precondition for this however is that clear rules are set up on the behavior in emergency cases which are reproducible for both isolated sides so the post-event development underground can be predicted by the rescue teams to a far most possible extend.

Emergency Situation Assessment bases on the following information:

1. The algorithm to locate the Center Node as described for the Topology Application (chapter 4.3) as the functional network describes the presumably accessible area to assign a meeting place, for evacuation or other activities. For this function the output of the topology application is available to the people underground on their personal devices (chapter 3.3.3) in form of a simple graphic (fig. 35).
2. The availability of audio communication on wireless devices (chapter 3.3.3) and using the hard wired loudspeaker and telephone systems in the area as far as accessible by the SIP service from the Center Node (chapter 4.5.3). This makes the people communicate with each other to personally assess the situation and all following actions.
3. Sensor information as far as available in the network (chapter 3.3.7) and resulting Emergency location detection support (chapter 4.5.1)

Basing on this information, most probably a safe place for all people to gather together has to be agreed. This can be any location in the mine, independently from the location of the Center Node or other network equipment: First Aid Station, Rescue Shelter, Supposed Emergency Exit etc. After mustering at this location, all people decide what do do and where to make an self escape try.

It showed that the details have to be decided and implemented individually for each mine

together with the safety authorities and (central) mine rescue organizations [19]. These algorithms then have then to be implemented in a mine individual underground Emergency Application as well as on the SafeCenter supporting the rescue teams so the probability of an efficient and quick success of a rescue action can be optimized.

This assessment will improve over time if the results from the analysis of earlier events are consequently transformed into enhanced algorithms and rules.

In so far, both server applications and Emergency Applications for underground have been implemented as a framework only top provide the basis for individual assessment functions and as a proof of concept.

4.5.3 Emergency Audio Communication

As soon as the Emergency Mode is established and the related services are started, all devices underground will be able to work in the network again, even if the switch over may cause some delay and service interruptions.

An important Emergency Application is the re-establishment of an audio communication. This is performed without any customized software implementation: On each MIC node the software of a SIP server is installed for use during Emergency mode when this service provided by the VoIPCenter server (chapter 4.1.7) becomes unavailable.

After the Center Node itself or one of it's neighbors have started the SIP service (chapter 4.4.2), a basic VoIP communication is available in the network covered area. The SIP server is configured to allow no dedicated phone calls:

In an emergency it is important that all people have the same information background. Therefore the SIP server is configured to accumulate all VoIP devices in one single conference group which is running in a mode reflecting the function of a walkie-talkie radio system. The disadvantage is that this procedure requires a basic communication discipline.

4.5.4 Meeting up

In case of an emergency it is essential that people in isolated working areas first gather together in order to assure everybody is there, to provide first aid to injured people and finally to decide about the further procedure. The related network supported procedures shall be explained by the help of an example:

A sample underground network layout basing on the Center Node evaluation example in fig. 36 is shown in figure 39 (modified from [125]). While the network cable in the tunnel at E1 was already disconnected before the accident (e.g. due to maintenance) it is anticipated that the exits E2 and E3 were disconnected in conjunction with an Emergency.

After the Emergency got known, the network determined the new Center Node as being *n3* in accordance with the implementation explained in table 9 in chapter 4.4.1 (marked CN in fig. 39).

For the external rescue teams a calculable behavior of the underground people is important now, so the rescue teams with a high degree of probability can assume what the people in the isolated area will be doing.

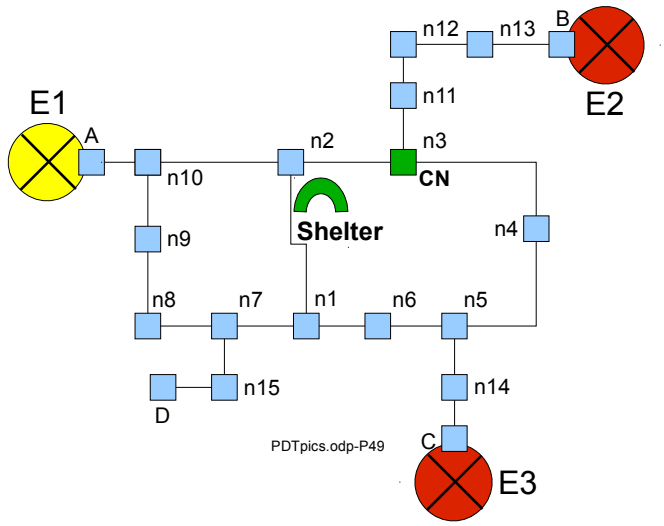


Figure 39: Isolated underground Network

Those however without being supported by the Safety Support Services of the network would not know anything about the situation. Now they get access to the following information which also is available to the teams above ground:

1. The potential exits 2 and 3 may be assumed blocked by fire gases reported by related environmental sensor values acquired by the MIC network nodes (see 4.5.1) and known to the above ground systems.
2. Some minutes after occurrence of the gases, the network dropped in the locations E3 and E2 which is known by the Topology Application (chapter 4.3) to all MICs underground and to the NetCenter server above ground.
3. From the tracking functions of the MICs it is known on the TrackCenter server above ground and to all MICs underground how many people were close to which network nodes at the time of network failure (chapter 3.3.5). From the history it is also known in what direction they potentially were moving.
4. Exit E1 is regarded available as the network link in this tunnel was down for maintenance when the emergency occurred.

All this information would not be accessible to the miners underground without having the network provided Safety Support Services available.

During the assessment of the situation (chapter 4.5.2), two alternatives would have been identified for the further procedure in this case, which also could be performed in combination with each other:

1. All people meet up at one central point in order to leave the area jointly (e.g. at the shelter close to the network node *n2*.
2. People located closer to the exit route number *E1* than to a central location (the shelter) are sent directly to the exit while the other from backward areas are meeting up first before exiting jointly.

For this example it is assumed that all people join up at a central location first (option 1, Shelter in fig. 40). However which routine is chosen depends on the underground distances and the actual situation!

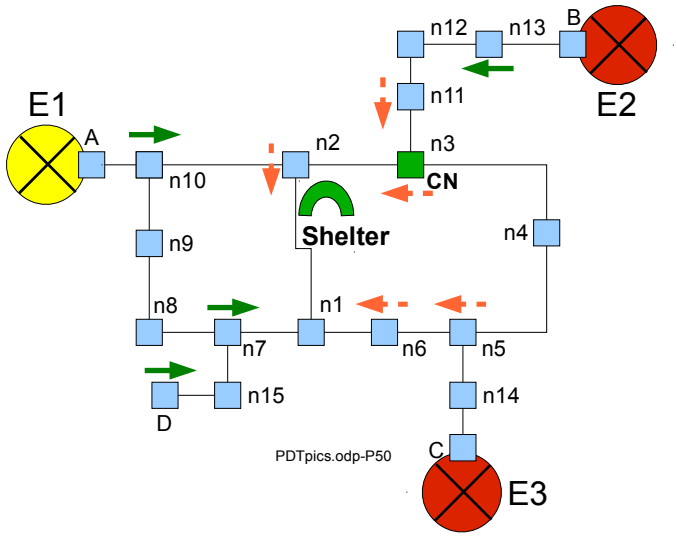


Figure 40: Guidance to the meeting point

To guide the people to the agreed meeting point the WLAN based tracking application on the MIC network nodes (chapter 3.3.5.1) provides the most important functions:

Each MIC knows from the internal tracking ring buffer in permanent memory how many WLAN devices are in proximity of this network node. From their MAC addresses the type of the device (handheld, machine etc) can be determined and finally concluded by the number of handheld devices, how many people are in the WLAN coverage area of this particular MIC network node. This information is then forwarded to related guidance clients on the personal devices (chapter 3.3.3) and to the LCD display on the MIC systems.

This information also includes the tracking data from the neighboring devices, so a MIC is able to track how many people (or handheld WLAN devices) are in the area behind towards the endpoint of the network.

In the example, the tracking application on the MICs and on personal devices guide the miners to the position of a shelter with the mobile personal devices working as "*underground navigation system*" with the addition, that the application shows to the miners whether there are people left behind in the area they come from. This information is injected from each MIC's tracking information (see 3.3.5). This is shown by the arrow colors in fig. 40: Orange means there are people in the area behind which could require a search before walking on or green means that the backward area is positively known as evacuated when no MIC shows handheld devices registered in the network behind towards the end point.

It is important that under normal circumstances – with all relevant information available to the MICs Emergency Applications – the recommendation of the Emergency Applications on where to meet etc. should be followed because then the rescue teams above ground can predict what the people are doing and prepare for related activities with highest priority instead of handling multiple scenarios simultaneously, a fact which speeds up action and prevents from unnecessary activities and prevents the rescue teams to be exposed to avoidable risks [98].

4.5.5 Self Evacuation

After all people are mustered at the shelter in the example explained in chapter 4.5.4, they jointly decide what to do next. Most probably they first will give first aid to injured people and potentially also search for missing people, if the situation allows.

Then the group jointly exits over one route (route 1 in the example). In other situations they may start investigating open routes or wait inside the shelter for rescue teams to arrive, depending on the situation.

4.5.6 Assisted Rescue

Before Assisted Rescue starts underground, the rescue teams above ground assess the situation separately in accordance to the procedures in chapter 4.6. The outcome are mainly organizational decisions about activities to be carried out. Therefore, the situation is best explained using the example in chapter 4.5.4 above:

In the example fire gases were reported at the routes to exits E2 and E3, so the central rescue teams most probably will start firefighting actions in these areas. For this they centrally analyze how the gas sensor values have developed and where the first network connection was

broken, what is traditional technology. This can be an indication for the origin of the fire which then is communicated to the firefighting teams.

As the routine proposed independently to the people underground (chapter 4.5.2f) is known above ground or can be simulated there, the rescue teams know that the people most probably will exit via exit No. E1. So at least on rescue team will be going down to meet with the group on route no. 1 or at the shelter.

When a rescue team then enters into an isolated area, they connect to the network island potentially using temporary equipment and power supplies (chapter 3.3.8) in order to inform themselves about the location of the people. Areas marked "*green*" mean to the rescue team, that they do not need to check those with first priority as these areas positively were reported clean of people. This helps the rescue teams by avoiding to spend time for searching in areas which are positively reported as evacuated. Thereby the rescue teams instantly can concentrated their work on those areas where presumably people are left who most probably need help.

4.6 Emergency Mode handling above ground

At the time of emergency mode declaration or detection, also the above ground systems, first of all the NetCenter is able to detect the situation by connection loss to the underground network components, as it does not receive Topology Telegram status updates from at least a part of the underground network any longer (chapter 4.3).

On the NetCenter the same Topology Application is running as on the underground MIC network nodes (chapter 4.3). This gives all above ground servers (chapter 4.1) a full picture of all pre-incident information of the situation underground. In contrast to the underground network however which homogeneously should consist of the MICs to actively participate in the safety support functions described in this document, the servers however can be located far away from the underground systems so on the way there may be non-MIC components (switches etc) used within the network. These units do not run the Topology Application (4.3). As they however are transparent to the protocol they simply will be ignored for the evaluation, but they do not block the algorithm (4.3).

During the Emergency Mode active in parts of the underground network, the above ground components, namely the NetCenter server mainly continue working as in Normal Mode. In the above ground Topology Application no dedicated Emergency Applications are configured to be started compared to the underground counterparts. Above ground applications mainly cover the notification of personnel about the event like a regular email, SMS or voice message alarm on the mobile phone.

In the servers all operational information nevertheless is logged in databases, so the evaluation of the situation can be carried our via the standard tracking applications available on the TrackCenter (chapter 4.1.5), potentially in combination with the mine visualization on the ViewCenter (chapter 4.1.8) and safety related environmental information from the SafeCenter (chapter 4.1.9) or dedicated, proprietary IT systems.

These safety situation analysis and visualization software applications are not part of this thesis. They may be subject to further research after the basic functions of this new Safety Support system have been proven.

While the Emergency Mode is ongoing, the NetCenter's topology application will recognize by incoming Topology Status telegrams from the formerly disconnected network nodes that the network or parts of it have reconnected. If this is the case, the operators are informed and

all information from the Emergency Mode is stored for later recovery and analysis before the System recovers to regular operation mode (chapter 4.7).

4.7 Emergency Mode recovery

Emergency Mode recovery (Sequence Numbers 4 in figure 28) is handled mainly by the underground components as there is no operational difference for the above ground installations.

The recovery also takes into account the fact that parts of the formerly disconnected areas can be reconnected randomly.

The detection of the network recovery is carried out via the Topology Status telegram transmitted regularly by the Topology Application running on all MIC nodes and the NetCenter server. For recovery, two situations have to be distinguished for the underground MIC network nodes and also for the underground network clients:

1. A part of the formerly disconnected underground network or a single node out of the network reconnects to the NetCenter, wheras none of the reconnecting MICs was operating as a Center Node.
2. A part of the formerly disconnected underground network including the Center Node or the Center Node solely reconnects to the NetCenter server.

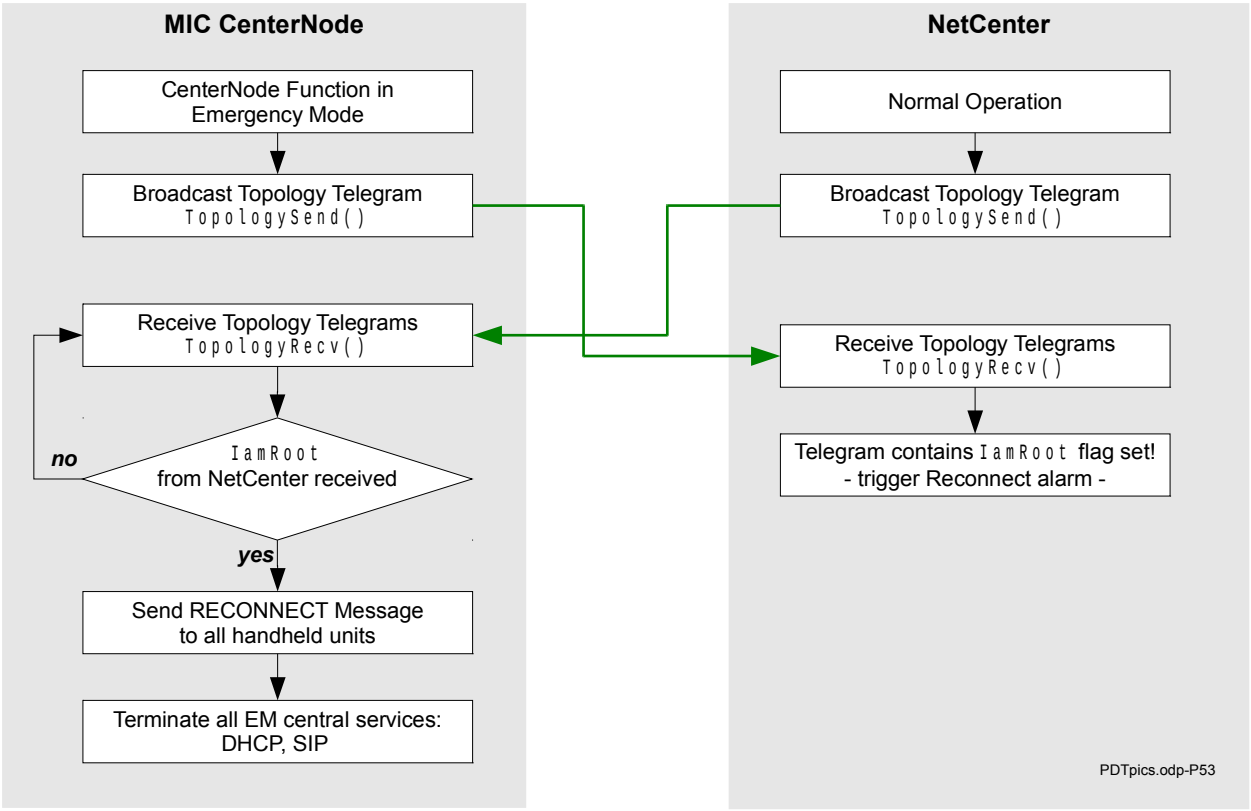


Figure 41: Reconnect Sequence triggered by the Topology Status Telegram

4.7.1 Network Nodes resuming Normal Operation

First the consequences on the reconnecting underground MIC network nodes has to be explained:

The first case does not provide an operational problem from the networking point of view, as it can be regarded identical to one or more formerly unpowered network devices newly entering the network.

In the second case it has to be made sure that there is no conflict between the central services like DHCP and SIP. This is resolved by the reconnecting Emergency Mode CenterNode as this node also receives the Topology Telegram message from the NetCenter including the NetCenter's "`IamRoot`" tag (fig. 41). The former Emergency Mode CenterNode then first sends a *Reconnect* message to all underground clients (see below).

After that, the node terminates all Emergency mode central services like DHCP server and SIP services, as they are available now from the central servers again.

Finally and in any recovery case, all reconnecting nodes freeze the history information acquired during Emergency Mode from all ringbuffers, especially tracking information, in non volatile memory to prevent this information from being overwritten. The frozen files are later sent to the SafeCenter for post event analysis of the Emergency situation [98].

4.7.2 Network Clients resuming Normal Operation

When the network resumes to normal operation, the client devices may be running on different IP addresses than those distributed by the NetCenter server. These addresses come from the same subnet, however are originating from the Emergency Mode space in this subnet as the were assigned by the underground MIC Center Node (chapter 4.4.3). For reconnecting to the above ground network this is not a problem, as all addresses still are in one and the same network. When after reconnection the lease of a client device expires, it will simply be renewed by the NetCenter DHCP server.

When a reconnect to the NetCenter is detected by the CenterNode as described in 4.7.1, all clients first are informed about the situation by the Emergency CenterNode issueing a *Reconnect* message as an application level message (chapter 3.3.2) to all handheld units to inform the users about the reconnect to the above ground units and to let them know that from now on for the next minutes some disturbance in network traffic may occur as the central

services are moved back to the above ground server systems.

Upon reception of a *Reconnect* message from the Emergency CenterNode address, the device freezes all emergency information gathered during the emergency and then restarts networking services (or reboots completely) with a "`ResumeFromEmergency`" Flag set. This completely cleans up the Emergency Mode and the device is forced to acquire a new DHCP lease, renew the SIP connections etc. When it then reconnects to the servers, the previously logged information is uploaded to the SafeCenter for potential later Emergency analysis.

The operational worst case of reconnection is the situation when the entire network including the underground Center Node is reconnecting (fig. 41), as this involves a Center Node message to be transmitted to the NetCenter and another Center Node message from the NetCenter received by all underground nodes.

In the first case the procedure is simple: Upon a command from the above ground operation center, the Emergency Mode is canceled and the Emergency Applications are stopped. Before these Applications are terminated, each application has to store a log file on the local memory media. A special program then has to assure that the local log file are transferred to the SafeCenter as soon a network connection becomes available later.

In case a network connection is available, the application has to store the related information directly on the SafeCenter server in the network.

After storing or sending the log files, the device potentially has to terminate or restart certain services so it runs on the regular network setup again, if the Emergency Mode was entered due to loss of above ground communications. This can also be handled by a regular reboot of the unit.

In general it has to be assured that the mode switching is performed in a minimum amount of time so it is performed with a minimum of operational impact on the mine.

Due to two networks joining in this case and potential network conflicts resulting from this situation, this step can be regarded non trivial, especially due to the fact that this switch-over should require a minimum possible amount of time (see chapter 4.7).

After returning to Normal Mode, all devices send logging information recorded during the Emergency Mode to the central Safety Center server in order to allow later analysis of the event. This transfer is performed by any device which was active during and aware of the Emergency Mode, regardless of being an infrastructure device or a field unit.

5 EXPERIENCE AND FUTURE DEVELOPMENTS

This chapter explains the tests and verifications of system wide relevance as well as operational experience with the system and it's implementation as described in chapters 3 and 4. It covers the MIC hardware testing (chapter 5.1), RSTP testing of the managed Ethernet switch (chapter 5.2), Wireless LAN underground coverage tests (chapter 5.3), System functionality testing (chapter 5.4), and a brief overview of the operational experience in the field (chapter 5.5).

Furthermore, the view of some safety authorities and related feedback is covered in chapter 5.6.

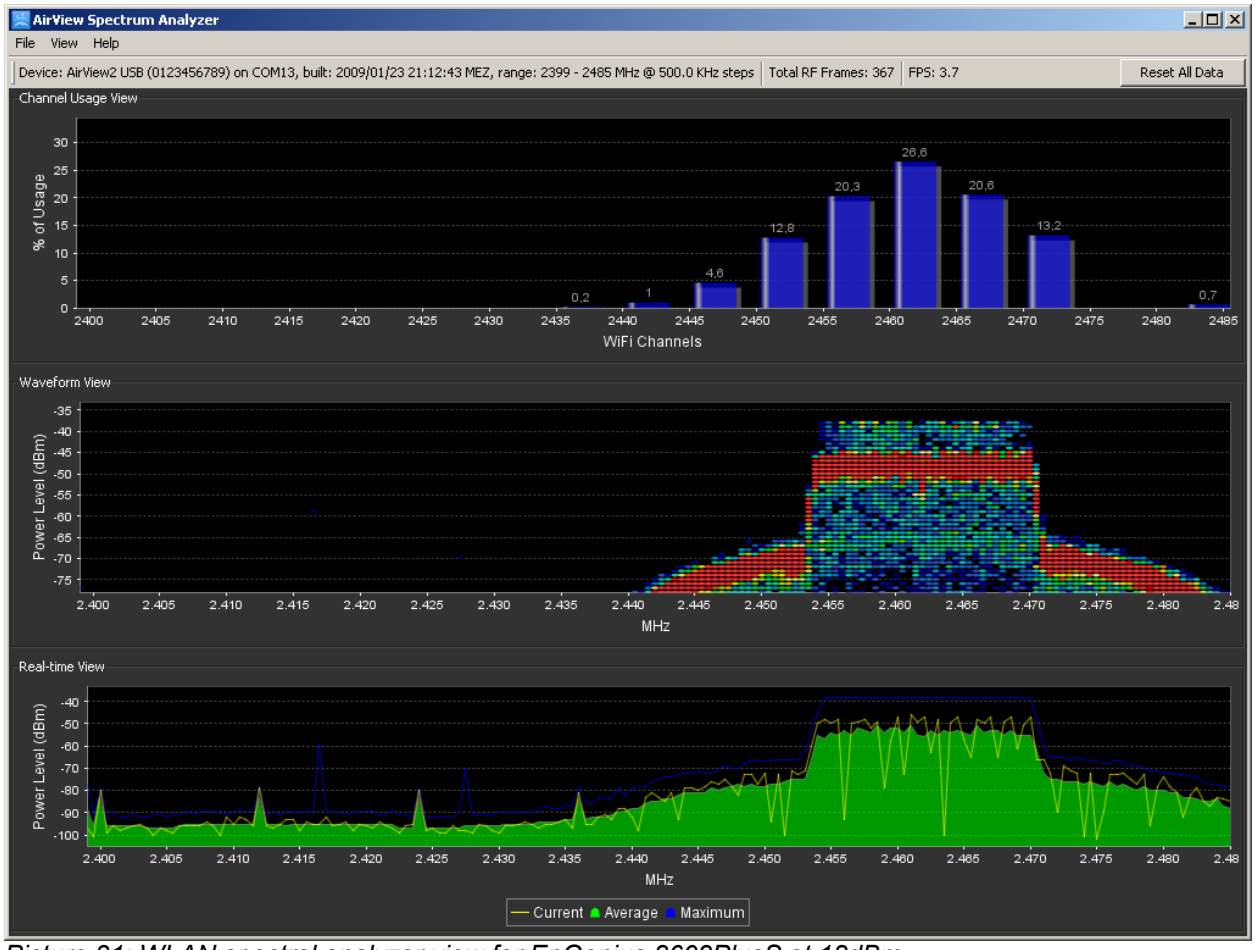
From all this experience significant needs for further research and improvements are resulting which can be found in chapter 5.7.

5.1 MIC hardware testing

The Mining Infrastructure Computer ("MIC") as the main infrastructure component is responsible for nearly all Safety Support functionality underground (chapter 3.2), which makes this hardware and it's reliability a critical hardware of system wide relevance.

5.1.1 RF hardware testing

One critical part in this testing was the RF behavior of the Wireless LAN transceiver cards used. Three industrial grade extended temperature range MiniPCI-cards with up to 26dBm transmit power were chosen for this laboratory scale testing. These were practical tests in a low RF contaminated (however non EMC chamber) environment accompanied by the use of a WLAN specific spectrum analyzer (*Ubiquity AirView*) [7]. A related picture for one chosen WLAN transceiver module is shown in picture 31.



Picture 31: WLAN spectral analyzer view for EnGenius 8602PlusS at 18dBm

The final transceivers were chosen basing on their RF performance to power consumption ratio in order to achieve the highest possible energy efficiency of the device [7].

5.1.2 MIC external Power Supply

The MIC devices have to be powered by different market available intrinsically safe (ATEX certified) power supplies. These power supplies differ mainly in their startup behavior, a technical parameter which is not stated in their data sheets but decisive to operate modern electronic not purely resistive loads. This behavior can also vary even between different revisions of one and the same product. Due to these facts, the use of the MICs was recommended only with the strongest ATEX power supplies available, which typically are limited to 2A at 12 VDC.

The power consumption of a MIC CPU module is dependent on the installed options. After optimizations during the design a fully equipped MIC is rated on a maximum operational current of 1.6A and an idle consumption of about 0,9A [175]. In order to minimize the startup current consumption, the different components of a MIC are started sequentially so the peak load is distributed to multiple peaks.

During start up of a second delivery of MIC nodes in RAG Anthrazit, the situation occurred that the units started with the old series of 2A ATEX power supplies but not with the new power supplies purchased for the new MIC devices. The same effect was measured when the devices were used with an Uninterruptable Power Supply (UPS) of the same manufacturer.

During a thorough analysis these startup problems were traced back to an extremely weak design of the power supply output which shows an extremely fast switch off behavior at nominal load rather than limiting the current and switching off with some delay. This is surprising

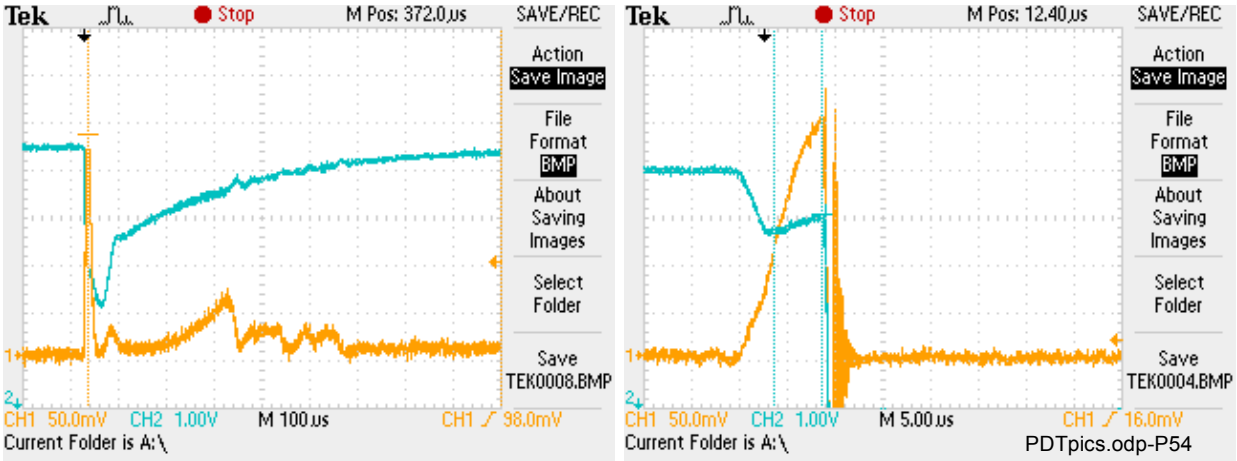


Figure 42: Start timing of SER power supply(left) versus Becker UPS (right) [136]

especially due to the fact that the MIC network nodes are able to start up with much smaller power supplies (SER, 1,4A nominal current, figure 42 left) compared to the UPS on 2,0A

nominal current. In Figure 42 (right) the cutoff of the questioned Becker-UPS upon MIC startup is shown [136]. This switching behavior at a cutoff-time of 2,5µsec makes it very hard if not impossible to be compensated by ATEX certifiable external devices.

For this reason, the design of the coming revisions of the MIC hardware was changed. In the new MIC150 revision of the device, the startup current is internally limited using TPS2421 current limiting devices designed for hot plug switching systems [158].

Another consequence from this experience also was to force the development of the MineTronics own Uninterruptable Power Supply (chapter 3.2.4.2) and an to complete the MIC system by an externally purchased regular power supply to prevent from such dependencies in the future.

5.2 Switch RSTP testing

During laboratory testing of the fiber optic switches an abnormal network behavior of obviously multiple spanning trees was observed in bigger meshed networks, which was analyzed closer.

5.2.1 Problem

In IEEE 802.1D-2004 RSTP [60], the parameter “Max Age” specifies the maximum number of hops a RSTP packet (“BPDU”) is allowed to perform in a network, or the maximum number of hops during that the BPDU information (like the Root Bridge ID) stays valid. Upon reception, each network node bridge increments the value of “Message Age” and checks it against the “Max Age”. If “Message Age” > “Max Age”, the BPDU is not going to be processed.

The “Max Age” value can be adjusted in a range starting from 6 going up to and including 40 (6 <= Max Age <= 40). The recommended default setting according to 802.1D-2004 is 20.

In case of RSTP, the network diameter must not exceed the Max Age parameter. If the diameter exceeds the “Max Age” parameter, the STA will elect multiple Root Bridges which results in the computation of multiple Spanning Trees that are not able to exchange any information. This is due to the fact that "*if the Port Receive state machine (17.23) receives an inferior RST BPDU from a Port that believes itself to be a Designated Port and is Learning or Forwarding it will set disputed (17.19.6), causing this [Designated port role] state machine to transition a Designated Port to Discarding.*" [60], page 177.

Consequently, the network diameter must not exceed the “*Max Age*” setting of RSTP! Further on, all switches should operate with the same setting of “*Max age*”. Note: Raising the “Maximum Age” parameter from the default of 20 to the maximum of 40 may introduce potential side effects that may require tweaking other parameters (e.g. “*Hello Time*”, “*Forward Delay*”) as well.

All path costs should be the same to maximize the number of reachable nodes. This can either be achieved by having the same link speed (e.g. 1Gbit/s) between all nodes or by manually setting the “Path Cost” to the same value for each and every link speed on all participating switches.

If a switch reports one of its ports to be in a state of “Designated Discarding”, it might be a sign for the existence of another Spanning Tree in the network [99].

5.2.2 Solutions

The aforementioned limits are due to the 802.1D-2004 RSTP standard, so there is no fully standard conformal software solution available [99].

The only really standard conformal solution is that a mining network has to be designed with respect to the resulting network diameter, which should not exceed 20. For this design, a related software can be implemented which, basing on the output of the Topology Application (chapter 4.3), could warn the if the network diameter is "*dangerously close*" to the "*Max Age*" parameter or even exceeds it. This tool could also be designed to support the customer designing the network in the first place, e.g. while using the ViewCenter 3D mine visualization software [99].

This fully standard conformal solution however limits the usability to practically very small networks as every single managed node will be counted a hop, even if this hop takes place between two switch modules inside one single MIC system (in the same underground location).

Consequently, an alternative solution has to be found. As all (RSTP based) failover functions are essential for the full functionality of the Safety Support system in bigger underground network installations, the final solution can only be to modify the RSTP configuration parameters as outlined above and test the results upon stability. This in turn requires access to the related firmware in order to be able to modify these settings and to verify that sides effects can be kept under control. For a related switch development, tenders have been carried out during the projects runtime which however did not show any big interest of industrial switch manufacturers to participate. Therefore, an in-house development of a managed switch module basing on a reference design and existing management software is planned for later in 2013/2014 to be able to provide all functionality required.

5.2.3 Hardware Field Testing experience

The first device was supplied to the RAG Anthrazit coal mine in Ibbenbüren, Germany in September 2010 for an early testing of the entire system stability and usability in the target operation environment. This initial system was also used for performing Wireless LAN coverage tests in this particular mine. The early installation date was possible as no completed ATEX certification was needed for this device as it is operating within the 150m distance from an air intake shaft, which allows industrial equipment without certification being used [79][74]. The main results of this early testing were [17]:

Picture 32: First MIC underground

1. The unit was working in a regular operational network to full satisfaction of the mine. In November, MineTronics performed a physical inspection of the device which confirmed full functionality, even of those parts, which are not used yet by the mine [17]
2. After installation the mine had some important comments on the usability and the functionality which immediately were taken into account in further development and certification. These ideas and recommendations mainly covered the following demands:
    1. Modifications in mechanical mounting the electronic modules inside the outer enclosure
    2. Installation of an LCD display in the outer enclosure door rather than using LED indicators
    3. Creation of a slave-switch module to achieve a larger number of fiber optic ports on the device

These requests were immediately taken into consideration and led to a additional small developments which were directly implemented into the device:

One main change and extension (no. 2) concerned the external display module which is a

monochrome matrix display using a white LED background illumination. This display in normal operation shows status information from all external interfaces and from the CPU. In Emergency mode, the display also is used to show situation dependent dynamic information e.g. to help under evacuation and to show directions to potential emergency exits.

The display is directly connected to the intrinsically safe general purpose I/O port used for the LED indicators, so hardware changes were not necessary.

The second extension (no. 3) resulting from this first operation experience covered an additional switch module which is connected to the MIC in order to provide a number of additional fiber optic or intrinsically safe copper network ports (chapter 3.2.3.7).

For the display and the integration of the slave-switch, certain software extensions and changes to the MIC firmware had to be made [17].

5.3 WLAN Coverage Tests

An essential part of the systems functionality comprises of mobile device functionality regardless of being for personnel tracking or for mobile communication. Therefore, the verification of the Wireless LAN behavior in underground infrastructures is an essential part of the entire system verification.

5.3.1 Test Equipment

For this WLAN testing, MineTronics uses a special test equipment which was created for this specific purpose in order to allow a practice related however reproducible WLAN performance testing in underground environments [93]. This equipment consists of:

1. A special software running on one or more MICs in the system
2. A backpack with a battery powered mobile MMG unit (chapter 3.3.4) and a mobile PDA or Smartphone device (chapter 3.3.3) as user interface.
3. A miner helmet with an omnidirectional antenna mounted on the helmet (
4. A distance measurement wheel assembly (like used by police to survey accident sites)

For the measurements, the MIC's are configured to run the measurement software which consists of an "*iperf*" server [81].

For the measurement, the MMG in the backpack is configured to run an *iperf* client set up to measure a bidirectional throughput of the link so both uplink and downlink can be evaluated. As antenna for the MMG the helmet antenna of the test person is used. While this person walks through the tunnel using the measurement wheel, the results from the *iperf* measurement are permanently stored to a csv structured file on the MMG together with the distance information acquired by two magnets on the measurement wheel resulting in one measurement to be stored every 500mm of distance walked. During the 500mm walk all single measurements performed by *iperf* are arithmetically averaged. At the same time

Picture 33: Test person equipped with measurement wheel and helmet antenna

the Wireless LAN signal strength values and the measured distance are stored in the csv file. All *iperf* measurements are performed using the udp protocol in order to be independent from link maintenance based issues during the measurements and due to the fact that udp also is the main protocol used in all MineTronics underground applications as well as for the Safety Support telegrams (chapter 4.3.4).

During the test, the test person uses the PDA or smartphone as a user interface which is connected via a different, non overlapping channel to the MMG in order to be able to read current values and to start / stop the measurement. Via the user interface also marks can be set which get part of the csv file in order to make special places during the walk part of the logging like transformer installations in the tunnel, a train, branching tunnels and other installations of potential influence on the measurement.

5.3.2 Measurements and results

This chapter outlines some exemplary measurements and their results in different underground environments at RAG Anthrazit Ibbenbüren, Germany, KWSA Bobrek Centrum Mine in Bytom Poland, OKD CSM mine in Karvina, Czech Republic and Premogovnik Velenje, Velenje Slowenia.

The basics of the WLAN behavior in tunnels is discussed in chapter 3.3.5.1 in conjunction with WLAN based tracking applications. All these applications basically run on the 2,4GHz WLAN channels in *IEEE 802.11b* but preferably in *g* mode. In order to prevent from disturbances caused by permanent mode and speed shifting, the maximum speed is set to 11Mbps. The impact of the transmit power used is relatively low. In these applications it seems to be much more important to use transceivers with best possible receive sensitivity available [106].

As this coverage is essential for all communication to safety relevant mobile devices, extensive tests were carried out. For the usage of Wireless LAN in tunnels, the following coverage situations have been determined:

1. Straight tunnel without any profile limiting elements along the tunnel axis
2. Straight tunnel with continuous profile limiting elements along the tunnel axis like a conveyor belt installation
3. Straight tunnel with single profile disturbances (branching tunnels) or profile limiting

objects (like transformers, vehicles, trains) in the coverage range where the tunnel extends again behind these elements

4. Curves and corners
5. Ventilation doors, often built as two door assembly ventilation locks

For all of those use cases, extensive practical tests have been carried using the measurement equipment explained above.

5.3.2.1 Straight tunnel

A typical signal and communication quality curve for a straight tunnel is shown in figure 43 [104]. This measurement run was performed with a single omnidirectional antenna setup on the MIC. The usable distance into one single direction from the MIC was measured with , whereas usability is defined as when the uplink data flow persistently falls below 1Mbps. In this measurement this is the case at about 170m.

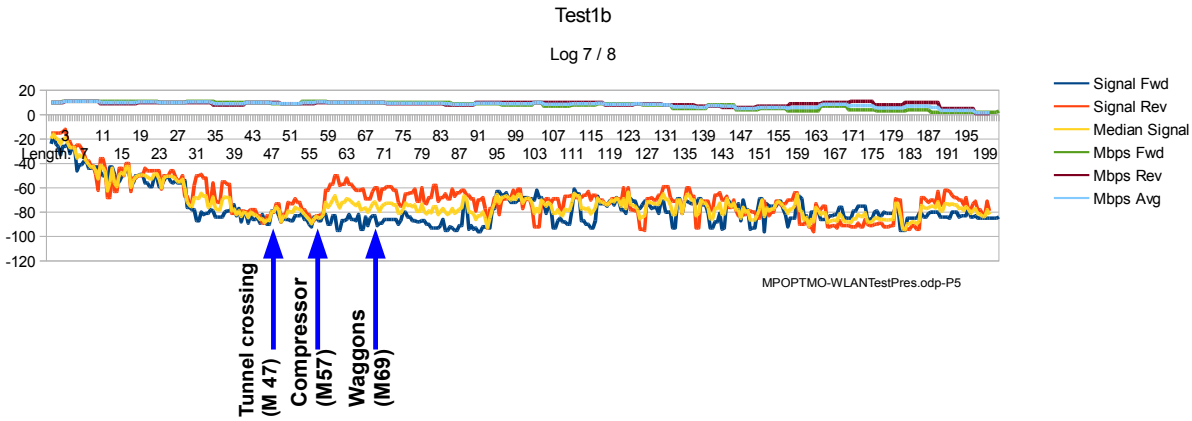


Figure 43: Measurement OKD: Straight tunnel single omnidirectional antenna

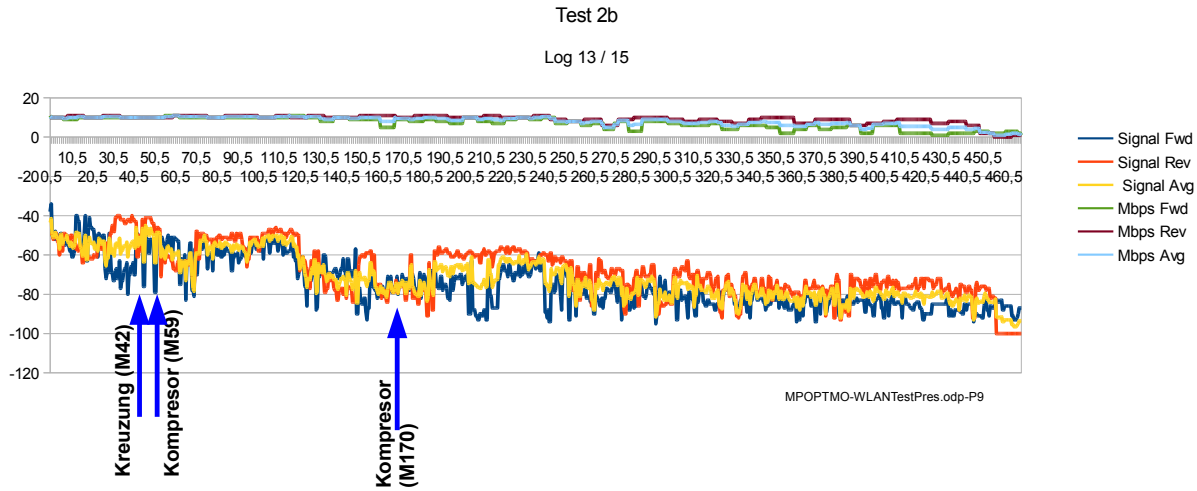


Figure 44: Measurement OKD: Straight tunnel double omnidir. antenna in diversity mode

In figure 44 the same measurement is performed using two omnidirectional antennas on the MIC in antenna diversity mode. This method pushes the usability range up to about 400m [104].

This effect was also confirmed in a nearly identical way at the tests at Premogovnik Velenje [105], even if there the tunnel profile was disturbed by a large conveyor belt installation, which matches use case No. 2 acc. to the definition above. This is shown in figure 45, where the usability limit in the two antenna layout (red and green lines) is at about 340m. Another result from this test was that a significant stabilization of the link (not necessarily a longer coverage zone) could be reached by mounting one antenna vertically in the side of the tunnel and the other horizontally in orthogonal orientation to the tunnel line or the tunnel wall [105].

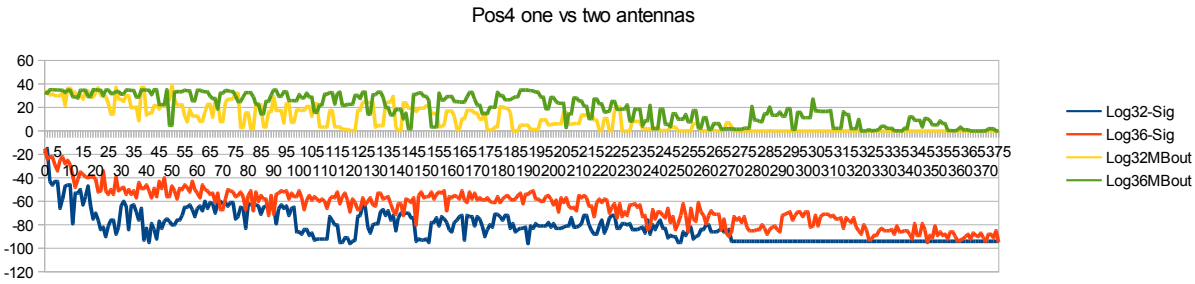


Figure 45: One antenna versus two in conveyor belt tunnel at Premogovnik Velenje

Another conclusion from this is that conveyor belt installations in a tunnel do not significantly reduce the WLAN coverage behavior in the tunnel. This conclusion is confirmed by measurements done earlier at RAG Herne [5] and RAG Anthrazit Ibbenbüren [106].

As antenna types in most tests both omnidirectional and sector antennas were used. Sector antennas with identical gain as stationary antennas did not show a significantly better coverage in propagation direction; However they only propagate in one direction while the omnidirectional antennas allow coverage to both tunnel directions. This is the reason why those are preferably used in practice. A practical reason for this similar coverage is seen in the fact that at some point the uplink from the mainly handheld client with built in low gain antenna becomes critical for the entire communication as the client is not able to create the waveguide effect in the same way as the stationary antennas. These impressions however need to be confirmed or invalidated by future research.

As it can be seen in fig. 43 and 44, single profile disturbances e.g. by objects placed in the tunnel like shown by the blue arrows in these figures are not significantly disturbing the performance. Due to the fact, that a full coverage of the profile very well ends up in a significant

impact on the signal attenuation it can be anticipated that this is valid up to a certain percentage of the tunnel profile. For a statistically safe determination of how exactly this influence is, further data from more tests has to be collected.

5.3.2.2 Curves and corners

Figure 46 shows a typical curve situation for an underground railroad tunnel where the measurement was performed in direction of *Test1a*.

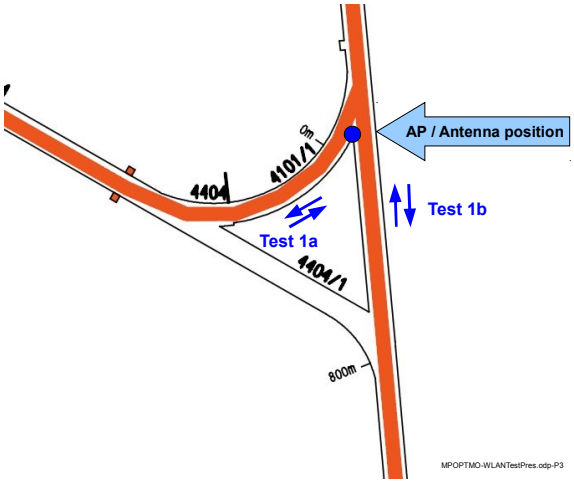


Figure 46: Test location Curve testing OKD [104]

The corresponding test results are shown in figure 47. From this measurement it can be concluded that the usability of this link ends at about 80 meters from the access point antenna [104] (fig. 47).

This result also matches other similar experience in other mining sites [5][107][106].

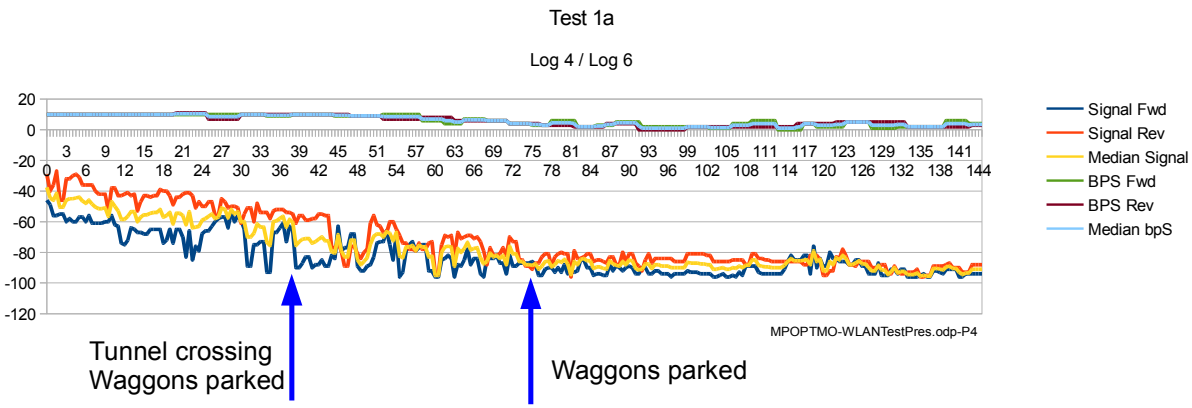


Figure 47: WLAN coverage around railroad track curve (Test1a) [104]

5.3.2.3 Ventilation doors

Ventilation doors are structures made from wood, steel or plastic materials which block the ventilation flow in a tunnel and are needed to keep the entire mine ventilated. Consequently most of these doors are arranged as ventilation locks comprising of a pair of two doors so only one door is opened at a time. Specific WLAN measurements were done for such doors at Premogovnik Velenje [105].

In figure 48 the opening of a ventilation door is shown while the WLAN cliens is standing in one single position 41,5 meters from the access point with a wooden ventilation door between

the WLAN client and the access point closed. At the time of the blue arrow the ventilation door is opened. The additional attenuation caused by the ventilation door hereby can be estimated on about 8 dB.

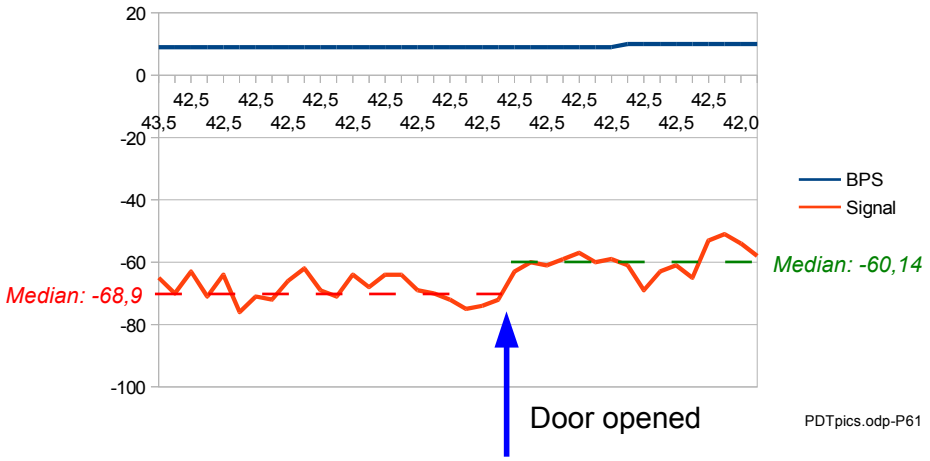


Figure 48: Opening of a ventilation door (wood) [105]

5.3.3 Recommendations

As a conclusion from the tests shown in the previous chapter, the following recommendations for the use of WLAN in underground environments are derived:

1. A dual antenna layout with antenna diversity or multi antenna systems (like in IEEE 802.11n) are very advantageous.
2. A dual antenna layout with one omnidirectional antenna mounted vertically and another one horizontally in orthogonal direction to the tunnel wall, the link stability is increased.
3. Directed antennas do not achieve substantially better coverage than similar gain omnidirectional antennas.
4. Objects placed in a tunnel do not significantly disturb the propagation as long as they do not exceed a certain percentage of the tunnel profile (like the full blockage by a ventilation door).
5. A coverage around a curve of about 80m can be expected. More coverage can only be reached by covering the curve with radiating antenna cable and place the radiator at the end of the cable instead using a terminating resistor.
6. Wooden ventilation doors may be calculated to cause an attenuation of min. 8dB.

5.4 System Functional Tests

During initial testing of the systems it has shown that the first approach of dividing the entire system into many small programs with well defined tasks with limited functionality leaded to a comparatively complex layout with a lot of internal communication inside the Safety Support system and with the underlying network services on the MIC node. During the first system tests it showed that this approach slowed down the overall verification and system development. In addition, the overall resource consumption (especially memory) was critical for the system to be run on small embedded devices.

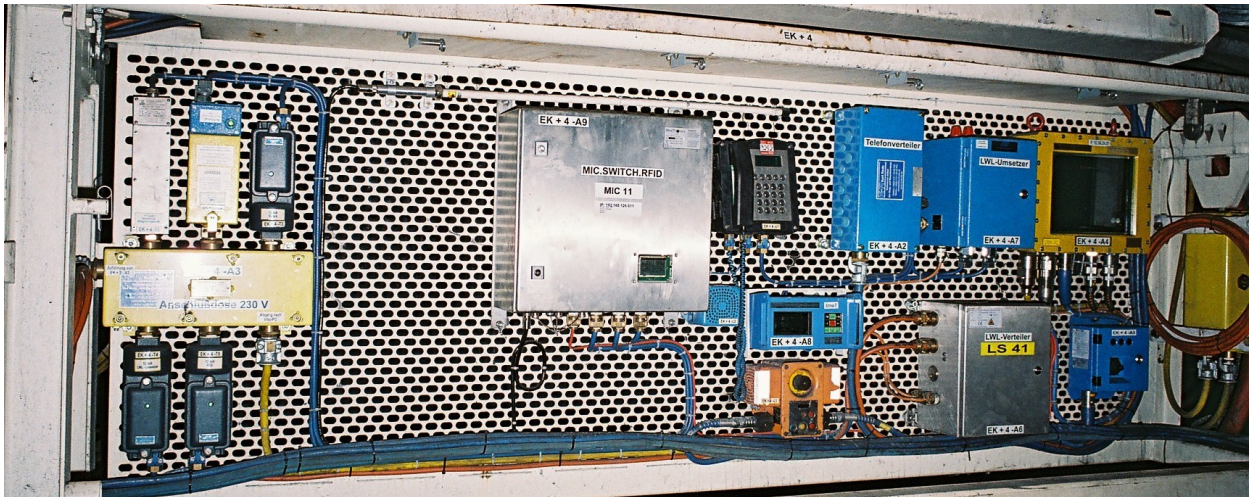
Therefore, the total modularity was reduced slightly by combining all crucial elements of the safety application inside the Topology Application. Now, the Topology Application runs all safety support functions except of the applications started during an ongoing Emergency Mode. These applications are launched by external scripts started by the Topology Application. It has shown that this approach consumes significantly less resources and provides a much cleaner and simplified handling within the application.

Thorough tests have been carried out to verify the creation of the network topology graphs and around finding the new Center Node as well as for switching to Emergency Mode. Most of these tests have been performed in conjunction with the switch testing as they are very closely related to the network hardware. During these tests also the RSTP problem reported in chapter 5.2 was detected and analyzed.

The mobile handheld clients (chapter 3.3.2f), namely pager and smartphone are functionally tested with their basic functionality needed for the Safety Support system, especially related to the Voice-over-IP functions of the smartphone and the messaging functionality on the pager devices. These tests were carried out in conjunction with the related Center software. For both handheld devices, the ATEX certification is pending, for the pager it is nearly completed. While by May 2013 the pager is commercially produced, the smartphone in it's basic functionality is released for sale in the fourth quarter of 2013, meaning that it soon will enter into production preparation.

5.5 Operation experience

The operation experience shows [136] [18] that Ethernet based underground communication systems are much better suitable and applicable for safety related underground communication than traditional communication systems as they are able to provide cabling redundancy and automatic failover functions as well as they are basing on well established international standards.



Picture 34: Final MIC assembly in underground operation at RAG Anthrazit [136]

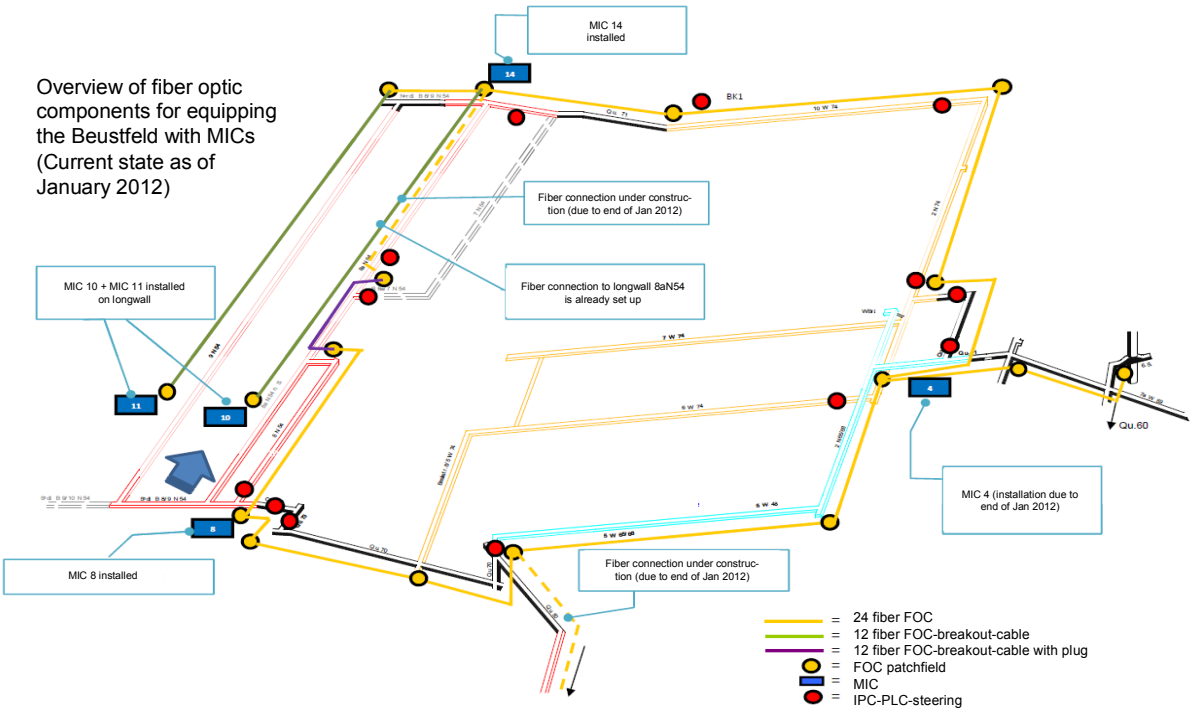


Figure 49: System status at RAG Anthrazit in January 2012

Weaknesses of the technology can be found in the area of WLAN coverage which is related to the Gigahertz range frequencies, where the coverage range inside the tunnels and especially around corners and curves is limiting the related RF distribution (see 5.3).

The MIC network node and fiber optic infrastructure systems are working reliably in underground mining environments at RAG Anthrazit Ibbenbüren GmbH since August 2010 [121] and since 2011 in other mines in Slovenia, Poland and the Czech Republic [136]. The status as of January 2012 in RAG Anthrazit is shown in figure 49. These systems are now gradually extended in order to finally also cover the Safety Support functions.

The extended use since 2011 also brought up some operational issues that needed to be addressed by going back to the design:

1. Older MIC systems reported heat dissipation problems as two or even three devices were mounted inside a single stainless steel outside enclosure.
2. Power supply problems due to Power Supply startup behavior (see chapter 5.1.2)
3. In some cases the SFP modules used in the switches were not building up fiber optic links any longer

The thermal issues were finally solved by introducing additional heatsinks inside the existing enclosures as a retrofit solution which was able to be applied in the field and finally by limiting the number of devices inside a single stainless steel enclosure to one main device plus one peripheral like a RFID reader and a VoIP converter.

The results of this modification is shown in figure 50, which shows the internal SFP fiber optic transceiver temperatures of a MIC system as logged by the mine's process control system. This system comprises of two devices in one system enclosure before enclosure upgrade on Feb. 06 2013 and after. The SFP temperature after the thermal upgrade finally stabilizes about 8K below the temperature prior to the upgrade.

As a consequence from this experience, newer generation MIC systems are built up in separate system enclosures per device and a total power dissipation limit of 20W inside one single stainless steel enclosure [136].

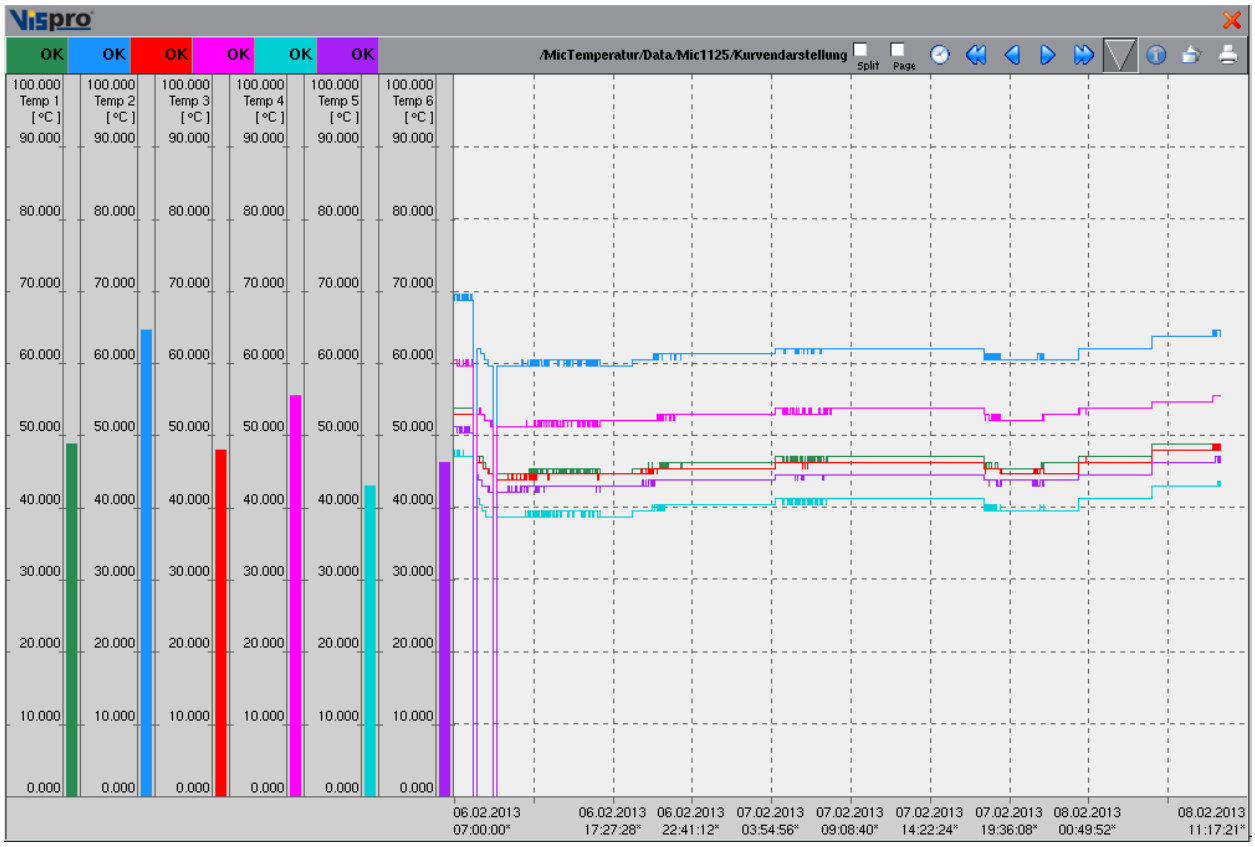


Figure 50: Internal SFP temperatures before and after thermal improvement [136]

The power supply problems (2.) have already beed discussed in chapter 5.1.2. As a consequence from those, the use of power supplies will be limited in the future to such delivered with the MIC systems.

Some operational problems occurred with few fiber optic links dropping out between the MIC network nodes. As this is an essential function for operational and safety purposes, this was analyzed very thoroughly. It turned out that the failure can be suspected to originate at a fast alternating power on / off of the devices caused by external ground failures in the specifics of underground electrical networks [74] which makes the circuit breakers to switch off when detecting the ground fault and on again after some seconds, then off again. To be able to verify this assumption, a specific test setup was created consisting of 20 switches and active fiber links on all ports. The switches were then power cycled in variable intervals between some msec and 10 sec and on different ambient temperatures between 20 and 65°C. The failure could be reproduced during this test, however a specific cycle time or temperature dependency could not be identified [174].

Further analysis of the defective SFP modules showed that the laser diode was working while an analysis of the communication of the SFP with the host switch was blocked after the

initialization packets were exchanged. The root cause of this failure was identified as a corrupted EEPROM on the SFP, which was caused by the host switch module overwriting it during the power cycle event. After discussions with the switch manufacturer, a new switch software was delivered which did not show any such abnormalities when the power cycling test was repeated [174].

Up to May 2013 the network based Safety Support functionality as implemented acc. to chapter 3 was positively verified mainly in laboratory scale as well as partly in major underground installations in four mines: RAG Anthrazit (D), OKD (Cz), KWSA (PL) and Premogovnik Velenje (SLO) still are ongoing [136]. When these installations are completed and run in regular operation it is expected that the Safety Support functions will be gradually introduced as they are part of an ongoing EU research demonstration project [136]. In this project ("OPTIMINE", EU RFCP-CT-2011-000001), different mining companies are implementing network based communication systems to enhance operational efficiency and underground safety [136]. The testing of the safety support features is one part of this project.

Due to the fact that up to now only ring structures were implemented in underground environment it has been difficult to proof in reality that the Emergency switching is working under all feasible circumstances. Therefore, the setup of a dedicated test environment is planned in a non Ex-exposed tunnel environment as a future activity resulting from the development works and also as a marketing site to demonstrate the functionality to potential customers.

5.6 The view of safety authorities

During the EMTECH R&D project a number of discussions was performed with the safety authority in Germany responsible for underground coal mining (*Landesoberbergamt NRW, Arnsberg*) and with authorities in Great Britain and Poland by the respective project partners [130][18][19].

These discussions originated in an early stage of the project in analyzing the weaknesses of the traditional communication systems (chapter 1.4.3.4) and setting up the criteria and demands on a future mine wide Safety Support communication system, expressed by key questions [19] to be covered by a new system:

- What if fire damages cables?
- What if a random section of roadway collapses?
- What if other physical damage occurs (e.g. caused by equipment)?
- What if a specified section of the mine floods?
- What if the power fails?

These questions all can be positively answered by the functionality of the new Safety Support communication system, which was highly appreciated by all safety authorities contacted.

An important result of these discussions was that the system is regarded complex and the correct handling in practice would be an issue for the workers on the mine. Therefore, a dedicated underground testing and training facility for such system would be essential to introduce the system in large scale in order to be able to thoroughly test new functions and software releases, as well as to train people in handling the Emergency Mode situations.

After the paper in the Engineering and Mining Journal [113] was published in the March 2013 issue, the author received an email correspondence from the head of the certifications unit at the US Mining Safety and Health Authority (MSHA) expressing strong interest in the technology and the possibilities for application in US American coal mines, which in turn also could lead to an official statement about the requirement of application. As however the certification rules are so much different in the USA, there is no attempt right now to certify the system for use in coal mining in the USA.

5.7 Future activities and outlook

The work performed in relation to this thesis has brought a substantial progress in application of standard network technology for supporting underground safety. The applications within R&D and public funded demonstration projects have shown that for a fully commercial application of this technology some further research and development activity is needed together with extended testing and verification:

The further extensions can be classified into a typical A-B-C schema as also all specifications in MineTronics are set up [98]:

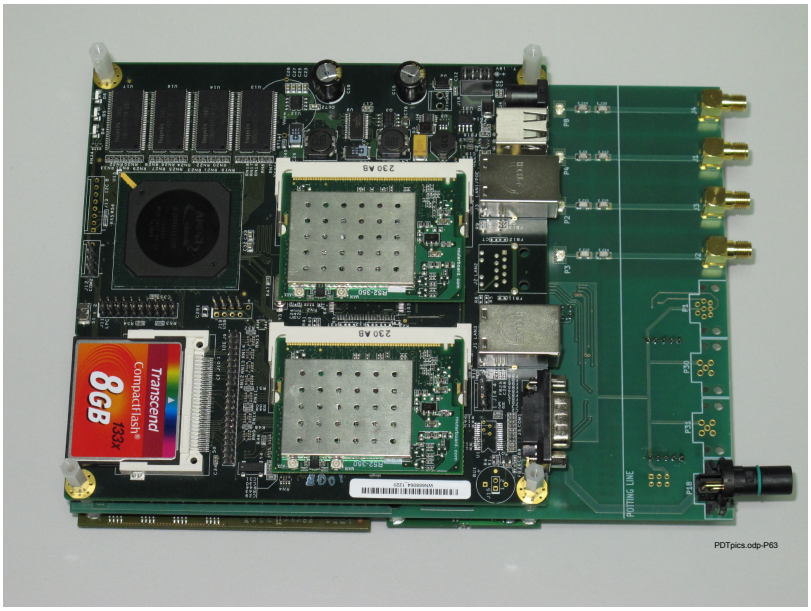
A = Improvements and activities which are necessary for a fully commercial application ("*urgent and important*")

B = Features needed for important options and addons ("*important but not urgent*")

C = Features which are improving comfort but not necessarily of commercial importance ("*neither important nor urgent*" or simply "*nice-to-have*")

5.7.1 Improvements for full scale commercial application

After now nearly three years of operational experience, the main infrastructure unit of the system, the MIC100 is just undergoing a major upgrade to a new revision (MIC150). This new device is already in production and by May2013 being introduced into first applications. The changes of the hardware included a new, more powerful CPU PCB, a new enclosure and a new Base-PCB for power handling and current limiting by special hot-swap controllers (chapter 5.1.2). This change also included major simplifications for the production process as well as for after sales service [88].



Picture 35: MIC150 electronics assembly

The implementation for showing how many miners are left in the area behind the current MIC towards the end point of the network currently has some weaknesses in the sense that it is not possible to include miners into the calculation which are temporarily out of WLAN network coverage, what is a quite regular use case. This is to be seen in conjunction with a much better communication between the MICs of the number persons left behind in the area. An ideal solution would be to add this information to the payload of the Topology Telegram, as an optimization of the Center Node finding algorithm (chapter 4.3) seems necessary in order to speed up Emergency Switching in future big networks: This includes an evaluation whether parts of the Dijkstra algorithm can be calculated permanently and made available via the Topology Status telegrams, so it can be prevented from every node recalculating the shortest paths for every node individually after a connection loss.

Another potential conflict needs to be addressed in a situation when the network nodes negotiate the new Center Node (chapter 4.4.2). In a bigger network and during a real emergency it can be anticipated that the network status is very volatile and dynamically changing, which leads to the fact that the network status on different nodes may be different resulting in different Center Node calculations which theoretically could end up in the fact that no Center Node can be assigned or a double assignment takes place (whereas the latter is cured by a timeout function). It has to be evaluated whether such situations can be prevented e.g. by freezing the network status upon connection loss to the above ground system for Center Node calculation. This however can have other disadvantages as it does not reflect potential further changes in the network right after the connection loss to above ground, which only leads to the possibility to delay Center Node finding by adding a timeout, if no further methods can be found during evaluation.

Further development work is ongoing in relation to the above ground server systems in order to enhance their usability with the Emergency Applications for underground use.

Generally, the Safety Support functionality has to be made more robust and reliable before being applied to commercial applications in final form. This relates to the implementation of additional error recognitions, adding watchdogs, alarms and also hardware indications on network nodes and especially includes a continued laboratory testing with a minimum of 15 devices involved.

5.7.2 Important options

As discussed in chapter 5.2, a limiting factor of the system right now is the network diameter as to the default setting of the MaxAge parameter in the RSTP protocol. To solve this essential demand for application in big underground networks, a new Managed Switch module will be necessary where all RSTP related parameters can be changed. Ideally this would be a custom design hardware basing on a reference design and an existing switch management intellectual property core (software). This also would enable an adjustment of the electronics hardware to the specific demands of the MIC products and simplify production.

Another alternative to a fully customized development would be the cooperation with a switch manufacturer, which would be preferred as it saves investment cost and development time. Such approaches however already have been done earlier when the original MIC was designed. However no supplier could be found who was interested in the comparatively small volumes needed.

It has to be evaluated whether the DHCP service on the MICs can be made working in a way so every MIC can be used as a regular failover peer after CenterNode negotiation in case of Emergency Mode. This would not require assigning DHCP addresses from a different range during Emergency Mode and would reduce the probability for IP address conflicts during the switchover between modes. This seems to be a bigger research task to find a solution which is as close to the standard as possible but provides a reliable and fast solution, which could be a typical subject for a continued academic cooperation, as also the RSTP handling described above. For this also extensive tests in a big installation have to be carried out.

An important additional Emergency Application would be to use the environmental sensor information available in the network and connected to underground locations to inform the people whether or not they have to use their personal oxygen masks or catalytic self rescuers. In this case the people can also be informed about the estimated time of use if they follow the evacuation route calculated by the system. This would mean that if this time is critical people rather quickly evacuate by themselves than spending time to search for others when they are exposed to the risk of loosing oxygen for themselves.

In the future, also the tracking data could be used for finding the most suitable meeting place by having the meeting place proposal algorithm minimize the total amount of distance to be walked by people underground so the meeting place will be in the area where most of the

people already are in conjunction with a potential route to an presumably available exit.

For route finding and evacuation purposes, the MEMS gyro in the smartphone and in the pager has to be integrated into the device functionality. The hardware is already part of the devices and this is proven functional. The implementation of the MEMS gyrpo is regarded an important option which can make guidance underground much easier. The development effort needed mainly consists of achieving the highest possible accuracy by applying related filtering algorithms, which also can take into account that the device is only able to move inside a tunnel, and the geometry and coordinates of this tunnel are known at least to the stationary network nodes.

A further important option is the automatic import of geospatial mining information into the above ground server systems. Because a mine infrastructure is permanently changing due to new tunnel excavated and new production areas taken into operation, the maps otherwise would have to be manually updated in regular time intervals (e.g. weekly or at least monthly). For an implementation, the use of related standards like the Geography Markup Language (GML) [85] would be highly recommended, as this is an open standard also subject to standardization in ISO TC211.

In order to use the system in full scale, training and testing software and simulation tools for emergency handling are precisely as important as to carry out real life trainings. For this purpose an easily accessible and non Ex exposed underground testing facility with a number of short tunnels interconnected in a complex layout would be ideal. In this layout about 20 network nodes should be installed with fiber optic links in between each other so any network configuration can be set up by remote device configuration reflecting all possible underground constellations.

5.7.3 Added Comfort

A simulator software for use above ground in case of an emergency for the behavior of the MIC systems underground and the safety related recommendations they would give in certain safety case scenarios would be very helpful for the rescue teams in order to predict the behavior of the people underground and the entire Safety Support system. This can then be used to a target oriented planning and performance of the external rescue operations. A precondition for such simulation however is that all kinds of scenarios can be tested in an underground test facility like described in 5.7.2.

5.7.4 Other activities

Other activities required for future following research include a thorough scientific analysis of the practical WLAN coverage tests in underground environments together with performing additional, target oriented tests with the goal of preparing a reliable guideline document which enables the WLAN design, in particular the positioning of the MICs and the antennas as well as the choice of the antennas to be predicted and designed right from the mine plans and tunnel geometries without performance of a previous specific site survey.

Further research is needed in the general and mine specific organizational handling of a major emergency. This is of special importance as once applied the new Safety Support communications have the potential to substantially change the working procedures in case of an emergency: This relates to new procedures and instructions needed for the behavior of people underground as well as for the Rescue Teams (see chapter 2.4.2.3 and 2.4.3). Also this part has to be seen in close conjunction with the training needed for the network based Safety Support System (see above). This emergency mode rescue handling however is not part of this implementation. This may be subject to more mining related coming research work, is however very closely related to the necessity of a dedicated testing facility (chapter 5.7.2).

Page intentionally left blank

6 CONCLUSIONS AND ORIGINAL CONTRIBUTIONS

This chapter contains a brief summary of the thesis, the major findings and an overview of the original scientific contributions of the author.

6.1 Summary

With the increasing demands on occupational health and safety and due to a number of major mining accidents involving people trapped underground it has been shown that conventional underground communication systems like telephones are not able to fulfill these demands any longer. This also relates to the fact that due to central above ground processing of all safety relevant data people underground do not have access to environmental sensor information when the communication lines to the above ground central systems get cut. In addition, mining companies today are obliged to fulfill the general legal obligations for safety and health which also would require to meet related demands on functional safety for such communication systems.

It was the goal of this thesis to demonstrate the feasibility of using extended Ethernet based network functionality to increase underground safety which on one hand has the capability of being certified to functional safety standards (like Safety Integrity Levels "*SIL*") and which on the other hand makes the network actively support the underground safety e.g. by keeping track of people's locations, by guiding people along the network to safe locations or to emergency exits and to advise about the underground environmental conditions on the evacuation routes.

The work related to the commercial developments and R&D projects this thesis bases on as well as the resonance from safety authorities have shown, that the idea of using an underground communication infrastructure both for mining operations and for safety support has the capability of significantly increasing underground safety without requiring substantial investments into a dedicated safety communication system [18].

This results in the implementation of a new Ethernet based communication system which provides multiple redundant link paths to above ground by using standard network protocols (like RSTP). In case of an emergency, where all connections to above ground get lost, the system automatically negotiates one network node to provide all vital network functions and emergency services. During an emergency the data from environmental sensors is integrated into the emergency functionality so people underground are able to investigate potential environmental dangers in the area around them.

The implementation comprised a complex multi disciplinary system involving electronics hardware development, software development, network and network security implementation and wireless RF technology, whereas always the organizational restrictions of underground

mining and the potential individual dynamics of an Emergency situation have to be taken into account.

This resulted mainly in a multifunctional use of network functionality extended by application level computing capabilities as a basic stationary infrastructure installed in the underground tunnels which is realized in special certified hardware. On every of these network nodes ("*Mining Infrastructure Computer*" - *MIC*), the algorithmic implementation of a network topology finding algorithm is implemented which permanently overlays the statically stored mine's tunnel layout with a real time network status so it is able to detect connection loss to above ground together with the location of the interruption as well as it is able to provide this emergency information to the underground workers. For this communication further components like mobile handheld devices have been realized.

The system was implemented during the work for this thesis with all major hardware and software components required to demonstrate the basic functionality as a proof-of-concept. This has been fully achieved by the application of the networks in several mines in Germany, Poland, the Czech Republic and Slowenia.

The proof-of-concept also showed that additional future work is needed in order to achieve a fully commercially usable status. This involves the need for a real life underground testing and training facility as well as improvements in the Topology determination and Center Node finding algorithms and additional emergency support functionality like e.g. using the semiconductor based gyroscopes already assembled in the handheld devices for additional guidance support.

Parts of this work were published on international conferences and in related journals which received respectable international resonance from potential users as well as from international mining safety authorities like from the Mining Safety and Health Administration (MSHA) in the USA. The key methods for the Safety Support systems are covered by the international patent application No. PCT/EP 2010/056825 (Patent Owner: MineTronics GmbH, Inventor: Christoph Müller)

The work related to thesis was performed in close conjunction with a research project about "*Emergency Support Technologies*" for mining co-funded by the European Commission's Research Fund for Coal and Steel ("*RFCS*") under the project No. RFCT2008-0001 and the project acronym "*EMTECH*". Parts of the testing and verification were performed within the

RFCS project No. RFCP-CT-2011-00001 "*Demonstration of Process Optimization for Increasing the Efficiency and Safety by Integrating Leading Edge Electronic Information and Communication Technologies (ICT) in Coal Mines*" under the project acronym "*OPTIMINE*".

6.2 Content of the Thesis and Final Conclusions

The first chapter "**Mining and Mine Communications**" introduces into the underground mining environment and mining safety before discussing traditional and unified network communication systems used in this environment.

Communication related safety regulations in Germany, the European Union and in the USA were analyzed upon compliance with today's regulations on occupational health and safety with the main conclusion that most of the current legislation concerning mine safety and communications was created and applied before standards and legislation relating to functional safety of technical installations became originally applicable in the late 1990's. Today, further norms and legislation apply which all together set high demands on the information of workers in case of accidents.

In order to analyze the resilience needed for an underground communication system an assessment of a Safety Integrity Level was performed resulting in a minimum Safety Integrity Level of SIL1, meaning that the communication system has to provide an overall availability of better than 99,9%. This assessment based on the recent German mining accident statistics. Such functional safety level cannot be met by any of the traditional communication systems like loudspeaker likes or telephones mainly. The reason for this is especially the robustness and redundancy of cabling and to the functional availability of these communication systems when the links to above ground systems are cut e.g. due to a tunnel collapse or a fire.

The required resilience however can be achieved by Ethernet infrastructures set up with redundant cabling by meshed and ring structures and by additional application level processing intelligence which assures local access to local information without intermediate above ground processing in case of a complete link loss to above ground.

The second chapter "**Safety Support for Mine Communications"** describes the main mine safety related functions originating from the Ethernet network or using it. This section mainly covers the general ideas and methods developed during the work on this thesis.

A main idea for many functions is to produce an electronic underground map basing on the geospatial tunnel layout with the network hardware layout and the positions of underground safety equipment as overlays to the tunnel map. This static tunnel map is available on all underground network nodes to provide independent location based services. Other dynamic overlays with real time information are created by each network node during runtime containing

the network link status information and the location of people as "*tracking information*".

When, in a worst case emergency situation the network link to the above ground servers is cut, the underground network basing on it's "*intelligent*" network nodes is able to detect the situation, switch to a special Emergency Mode and thereafter to maintain all emergency relevant network services. Additionally, the location of the link loss may be interpreted as the location of the emergency when e.g. a cable was destroyed by rockfall or fire.

One of the network nodes in the center of the network ("*CenterNode*") is determined to provide central network services so the basic network functions e.g. for address resolution are available.

Each worker underground is equipped with mobile electronic devices so he can be tracked e.g. via the mobile device association with a WLAN access point in each network node. Dependent on the information about the location of the miners, the location of safety equipment and the personal subjective assessment of the situation the miners can communicate in the functional network and decide upon a meeting point. During their walk to the meeting point the network nodes are virtually guiding the people basing on the stored tunnel and network maps. When they pass a network node, the network node also is able to tell them whether or not people are left behind so it is assured by positive assessment that the entire area is completely evacuated. After people met they may decide to evacuate using their handheld devices in dialog with the network node in order to find an exit which dependent on the actual situation should be accessible. As long as these computations are basing on the information available in identical form on above ground servers at the time of the accident, above ground systems are able to simulate the proposals of the underground network nodes so the assisted Search-And-Rescue can be organized with a very high efficiency and minimized risk for the rescuers.

Chapter three explains the "**Implementation of the underground hardware".** This section gives a general introduction into the system implementation and explains in detail the realization of the stationary network infrastructure hardware and the mobile application devices which are used underground.

The entire system including above ground and underground systems has to implement four use cases: Configuration after component startup, regular operation with all parts functional, Emergency Mode operation isolated underground and Emergency Mode operation isolated above ground. This also leads to the working cycle with Regular Mode, split processing in Emergency

Mode and Recovery to regular mode.

The main device is the "*Mining Infrastructure Computer*" ("*MIC*"), which combines an embedded application CPU, a managed fiber optic switch and two wireless LAN transceivers and a custom developed base board containing Ex certification relevant safety circuits and a microcontroller to supervise the unit and to handle external peripherals as well as the internal power up sequences. All device is mounted in a steel enclosure and encapsulated in silicone compound for Ex safety. Together with separate peripheral devices like additional switch or RFID readers this conforms a system completely mounted in a stainless steel enclosure.

To be able to supply the unit with battery power backup, a fully intrinsically safe Uninteruptable Power Supply (UPS) system was designed and prototyped. This included the development of a smart intrinsically safe battery pack of 10Wh which is multiply used inside the UPS to provide up to 240Wh. The battery pack is already used in commercial applications within a third party automation system.

The mobile application devices include a WLAN pager and a smartphone like device. Both are using inductive charging and the battery technology which also is used in the UPS battery pack. The pager's main component is a "*Flyport*" WLAN module with PIC microcontroller, while the phone bases on a system-on-module containing an OMAP processor CPU. The phone also can be equipped with an optional 1,2 Mpix camera module. Both units have optional accelerometers (pager) and a MEMS gyroscope (phone) which later may be used for guiding and dead man recognition functions.

These WLAN devices are the basis for the people tracking functions and for extended use of those in e.g. gate applications for access control to dangerous areas. WLAN tracking is implemented in the MIC's by analyzing the association and the WLAN signal strength data. From this, XML Web Service based telegrams are sent to the TrackCenter server above ground.

Chapter 4 illustrates the "**Implementation of Central Systems and System Functionality".** This chapter explains the implementation of the central systems needed above ground and the functionality of the Safety Support System.

The server functionality is split into several *Center* applications which either can be run as virtualized LINUX servers on a single server hardware or on dedicated servers. The operating system is prepared for clustering hardware in order to provide a full and immediate system redundancy. The server applications are basing on Java 2 Enterprise Edition using a MySQL

database. The tasks are distributed in the way that the *NetCenter* handles all configuration and device administration, the *TrackCenter* is dedicated for logging all tracking data and performing tracking related applications like the WLAN access gates, the *PagerCenter* handles the text message exchange and the *SafeCenter* takes care of all safety related information.

A fundamental function for most Safety Support functions is the permanent observation of the network topology status and the availability of this status information in all *MICs*. This is implemented by a "*Topology Application*" running on all *MICs* and on the *NetCenter* above ground. This application collects status information on the hardware address of the remote neighbor connected to each port of the switches mounted in one *MIC* system. For this determination the LINUX shell command *snmpwalk* is used. This information is part of a very small and low impact *Topology Telegram*, which is an UDP telegram distributed in the network using multicast or broadcast methods. As the *NetCenter* above ground is running the same application, it automatically gets informed about the status of all devices underground and their neighbors. The telegram is part of sensitive safety functions, therfore it is secured and authenticated.

From this *Topology Telegram* data, every single *MIC* creates a linked *NetNodeList* with one entry for each *MIC* in the network and it's neighbor addresses. From this list each *MIC* network node is able to create a full real time link and node status matrix of the network. To create graphic network overviews on the *NetCenter*, the matrix is exported to external programs in XML format.

An Emergency Mode situation is detected by all nodes individually through the loss of contact to the *NetCenter*. This is the case, when the *NetCenter* does not send any *Topology Telegrams* which at the same time also contain the "*IamRoot*" flag set. In order to keep the routine independent from a certain address, the *MICs* interpret the fact that nobody has set the "*IamRoot*" flag to initiate Emergency Mode. After the Emergency Mode is detected, the remaining *MICs* in the isolated network start negotiating the new CenterNode. CenterNode is defined as the network node with the most equal number of network connections ("hops") to all end nodes in the network. From it's *NetNodeList*, every single MIC individually runs the Dijkstra algorithm to determine the shortest path of all nodes inside the network to all endpoints of the network. From this calculation every single node creates a similar matrix containing the number of hops from each node to each endpoint. The node with the lowest standard deviation from the average number of hops to all end points declares himself the new CenterNode providing the

central network services by starting the *DHCP* server and e.g. SIP for VoIP communication or application services like running the web server for the environmental data.

The further procedure in emergency is a combination out of organizational and technical implementation: First, people underground access the environmental sensor information and the safety overlays of the tunnel map in order to assess the situation and make a decision most probably about a suitable meeting point. Then this decision about a meeting point is communicated via voice communication which is configured to couple all devices in a "*walkie-talkie*" radio mode, so one speaks and all others listen. If the meeting point also is entered into the system by declaration of the closest *MIC* as "meeting point" the other *MICs* are able to guide people along the network to this place. By counting the personal devices associated with one single *MIC* each *MIC* can also state whether or not people are in proximity. Using this information, it can be assured and positively signalized to the people whether or not certain areas are evacuated. The same procedure can be used for a following self evacuation when people are walking to an emergency exit.

Recovery from Emergency Mode is initiated as soon as the formerly isolated MICs start receiving "*IamRoot*" flags from the *NetCenter* again. In this case the Emergency Mode *CenterNode* issues a *reconnect* message to all client devices causing them to restart their network services and then terminates the central services in order to resume operation in regular *MIC* mode.

Chapter 5 explains **Experience and Future Developments.** This section contains statements about tests performed and the operational experience with the implemented parts of the system and conclusions together with an outlook onto upcoming research and development.

Intensive system integration testing showed startup problems with certain Ex certified power supplies, which are designed not to limit the output current when startup current spikes occur but switch off the power supply. This resulted in a design change for the future MIC generation which is extended by a fast internal power limiter chip.

When testing big meshed networks in laboratory scale multiple spanning trees were observed. The cause was found in a limitation of the RSTP "MaxAge" parameter, which specifies the maximum number of hops a RSTP packet ("BPDU") is allowed to perform in a network leading to the fact that the network diameter of active RSTP devices may not extend the MaxAge parameter which is taken into account when designing networks today. However for

future bigger networks some intensive research is needed about the side effects when this parameter is increased specifically for this application.

The hardware testing was performed in mining applications in Germany, the Czech republic, Slowenia and Poland. It showed that the thermal behavior of the system enclosure needed to be modified for hosting multiple modules. Furthermore, customers also initiated detail enhancements like an LCD display for the MIC system.

As WLAN coverage is an important precondition for system functionality, extensive field surveys were carried out in all mines operating the units. In all these surveys it can be concluded that the signal degrades rapidly in a near field of about 30-40m from the stationary antenna similar to an attenuation curve in free field. It follows an area of up to several hundred meters in a straight tunnel where the signal does not seem to attenuate. This effect is described in literature as "*waveguide effect*" in which the multiply reflected, scattering signal waves are "*guiding*" the direct wave through the tunnel. This way usable coverage ranges of up to 400m into one direction from the MIC have been measured.

Future improvements are already started with the design and production of the MIC 150 device which incorporates enhancements of the baseboard, a new CPU board and production related improvements.

The operation experience also has shown that certain improvements to the Topology Telegram will be advantageous as e.g. communicating the number of people associated to one access point to it's neighbors in order to enable them to directly show the number of people left behind without requiring a separate communication. In a bigger network also the determination of the CenterNode will take significant time as every node has to apply the Dijkstra algorithm for each node in the network and each end point individually. For another potential improvement it has to be researched whether the DHCP service on the MICs can be made working as a regular failover to the primary server after the Center Node is determined. Further improvements are implementation related and cover e.g. the use of the accelerometers and gyroscopes in the handheld units as well as improvements of user interfaces.

6.3 Original Contributions

The following contributions are original work the author performed himself in conjunction with this thesis:

6.3.1 Theoretical Contributions

6.3.1.1 Performance of Studies

- Study on status quo of mining safety regulations connected to communications (chapter 1.2)
- Study on communication related consequences from mining accidents (chapter 1.2.5)
- Study on an application method for Safety Integrity Levels for underground communication systems (chapter 1.3)
- Summarizing study on the traditional communication systems in use (chapter 1.4.2)
- Planning Questionnaire and user survey on safety relevant mining communications in use and their resilience as part of the study on traditional communication systems (chapter 1.4.2)
- Analysis on the Status Quo and resilience of traditional underground communication systems (chapter 1.4.3)
- Analysis and summary of international studies on mine communication resilience (chapter 1.4.4)
- Study on early unified mining communication systems (chapter 1.5)
- Study on safety related Ethernet architectures and their SIL compliance (chapter 1.6.1)
- Derivation of criteria for safety related underground communication systems (chapter 1.6.2)
- Status and extend of use of Ethernet as underground mine communication systems (chapter 1.7)

6.3.1.2 Critical and comparative analysis

- Analysis of resilience of traditional communication systems versus Ethernet based infrastructures (chapters 1.4.3.4, 1.6.3)
- Analysis of conventional communication system legislation compliance upon compliance with functional safety regulations (chapters 1.3, 1.4.3
- Analysis of tunnel availability for evacuation by link status evaluation (chapter 2.3.5)

- Analysis of high level use cases of the entire safety support system and their interconnections(chapter 3.1.1)
- Electronics analysis upon ATEX certification compliance and related calculations (chapters 3, 4, 5)
- Analysis of WLAN coverage test results and derivation of operational consequences and recommendations (chapter 5.3)

6.3.2 Contributions to Fundamental Research

- Method of using Ethernet as a highly resilient, meshed communication infrastructure to reflect the geospatial mine layout (chapters 2.1.1, 2.1.3)
- Method of using the network as overlay to the tunnel layout in order to derive location and safety information (chapter 2.2.2)
- Method of using safety equipment locations as overlay to the tunnel and network maps (chapter 2.2.3)
- Method of detecting emergency locations by unavailability of network links in timing context to an emergency or in conjunction with safety relevant sensor information (chapter 2.3.4)
- Method of storing all static safety related information incl. the tunnel and network topologies on every single network node to derive safety support information (chapters 2.2.1)
- Method of using link status information as trigger criterion for emergency detection (chapters 2.3.1ff)
- Method of using the link status to find available emergency exits (chapter 2.3.5)
- Method of local (underground) processing of tracking information and storage in the network nodes for server-less availability of people location information (chapter 2.4.1)
- Method and procedures for network supported dynamic evacuation (chapter 2.4.2)
- Optimization of methods for support of external rescue by use of tracking information (chapters 2.4.3.1, 2.4.3.3, 2.4.3.4)
- System for temporary rescue team network setup (chapter 2.4.3.2 and 3.3.8)
- Use and Purpose of above ground server systems (chapter 2.5)

The key parts of these ideas and methods developed as original contributions are covered by the international patent application No. PCT/EP 2010/056825 (Patent Owner: MineTronics GmbH, Inventor: Christoph Müller)

6.3.3 Contributions to System Implementation and Testing

- Creation of system functional and hardware specifications for all devices stated (chapters 3.1.2, 3.2, 3.3)
- Overall system architecture (chapters 3.2.1, 4.1.3, 4.2)
- ATEX type approval related design and related reviews for the electronics and electromechanics implementation of all underground hardware (chapters 3.2, 3.3)
- ATEX type approval document setup for the underground hardware in chapters 3, 4, 5)
- General architecture and design framework of the UPS and intrinsically safe battery pack (chapter 3.2.4)
- General architecture and concepts of the Pager and phone devices, charging station in common form factor with smartphone and pager messaging functionality with pre selectable answer routine (chapter 3.3.2 and 3.3.3)
- Architecture and design of the tracking processing and WLAN antenna gate function (chapter 3.3.5)
- Architecture and design of the NetCenter, TrackCenter and SafeCenter server systems with important input on system distribution, internal communications and failsafe configuration and software upload to underground embedded systems (chapters 4.1.3, 4.1.4, 4.1.5, 4.1.9)
- Architecture and methods of guidance and integration of the location based 3D visualization engine into ViewCenter (chapter 4.1.8)
- High level functional design and message data flow for the pager application software (chapter 4.1.6)
- Architecture and Design of the high level working sequences and functions for the Emergency Mode switching and the Safety support functions (chapter 4.2)
- High level architecture of the Network Topology determination and Emergency mode detection functions (chapters4.3 and 4.4)
- Architecture and high level design of the Emergency Applications (chapter 4.5), the Emergency Mode handling above ground (chapter 4.6) and the recovery (chapter 4.7)
- Planning and performance of WLAN RF and coverage testing (chapters 5.1 and 5.3)

Page intentionally left blank

Bibliography

1 ABB, *Industrial Ethernet: Auf dem Weg zum Industriestandard - Volume D/E*, Würzburg: Vogel Verlag, ISBN 3-8259-1910-2, 2001

2 Aho, A.V., Kernighan, B.W, et al, *The AWK Programming Language*, Boston, MA, USA: Addison Wesley, ISBN 0-201-07981-X, 1988

3 ATMEL Corporation, *ATMEGA Microcontroller Datasheet*, San Jose, CA, USA: 2006

4 Bauer, J., *OpenVPN*, Heidelberg, Germany: dpunkt.verlag, ISBN 978-3-89864-396-2 , 2006

5 Bergmann, S. and Mueller, C, *Felderprobung von WLAN Infrastrukturkomponenten*, Ladbergen, Germany: Embigence GmbH 2004

6 Biro, G., *MineTronics C/C++ Coding Standard for Embedded Systems*, Ladbergen, Germany: 2010

7 Biro, G., *Mini PCI card RF test report*, Ladbergen, Germany: MineTronics GmbH 2009

8 Biro, G. and Mueller, C, *Safety Underground Network Systems: Topology Application*, Ladbergen: MineTronics GmbH 2011

9 Biro, T., *MIC1 RFID Hardware User Manual*, Ladbergen, Germany: MineTronics GmbH 2011

10 Biro, T., *MMG1 User Manual*, Ladbergen, Germany: MineTronics GmbH 2010

11 Biro, T., *Net Center User Manual*, Ladbergen, Germany: MineTronics GmbH 2012

12 Biro, T., *PAG1 Pager/Messenger Device User Manual*, Ladbergen, Germany: MineTronics GmbH 2012

13 Biro, T., *Pager Center User Manual*, Ladbergen, Germany: MineTronics GmbH 2013

14 Biro, T., *Track Center User Manual*, Ladbergen, Germany: MineTronics GmbH 2012

15 Biro, T., *VoIP1 Gateway User Manual*, Ladbergen: MineTronics GmbH 2012

16 Brenkley, D., *EU EMTECH Project: Mid Term Report*, Brussels, Belgium: 2010

17 Brenkley, D., *EU RFCS EMTECH Project: 5th Semester report*, Brussels, Belgium: 2011

18 Brenkley, D., *EU RFCS EMTECH Project: Final report*, Brussels, Belgium: 2012

19 Brenkley, D. and Mueller, C, *Safety Assessment Methods for Mining Communication Systems*, Brussels: Mines Rescue Ltd / MineTronics GmbH 2010

20 Brenkley, D. and Müller, C, *Communication system resilience*, Brussels: Mines Rescue Services Ltd / MineTronics GmbH 2010

21 Bundesministerium für Wirtschaft und Technologie, *Der Bergbau in der Bundesrepublik Deutschland 2009*, Berlin, Germany: Bundesministerium für Wirtschaft und Technologie 2010

22 Chen, G., *XCenter System Architecture*, Ladbergen: MineTronics GmbH 2010

23 Chinnici, R., *Web Services Description Language (WSDL) Version 2.0*, : Sun

Microsystem (W3C) 2007

24 Chinnici, R., *Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language*, : Sun Microsystem (W3C) 2007

25 Chirdon, D., *Emergency Communication and Tracking Committee Underground Communication and Tracking Systems Tests at CONSOL Energy Inc., McElroy Mine*, Washington DC USA: 2006

26 Deutsches Institut für Normung (Ed), *DIN EN 60079-0 Explosionsgefährdete Bereiche - Teil 0: Betriebsmittel - Allgemeine Anforderungen*, Berlin, Germany: 2013

27 Deutsches Institut für Normung (Ed), *DIN EN 60079-11 Explosionsgefährdete Bereiche - Teil 11: Geräteschutz durch Eigensicherheit "i"*, Berlin, Germany: 2012

28 Deutsches Institut für Normung (Ed), *DIN EN 60079-25 Explosionsfähige Atmosphäre - Teil 25: Eigensichere Systeme* , Berlin, Germany: 2011

29 Deutsches Institut für Normung (Ed), *DIN EN60079 Explosionsgefährdete Bereiche - all parts, German Edition*, Berlin: 2013

30 Dijkstra, E.W., *A Note on Two Problems in Connexion with Graphs*, Numerische Mathematik, 1, (7): p 269-271, 1959

31 Draeger Safety AG, *Communication Mask Draeger*, Lübeck, Germany: 2010

32 ECOM GmbH, *ECOM product range PDA*, ECOM GmbH, online available on: 30.12.2010 at http://www.ecom-ex.de/produkte/mobile-computing/pocket-pc/iroc/geraete/iroc-620-ex-serie.html. Accessible in file: Iroc620-ExSerie.pdf, 2011

33 Einicke, G., *Proximity Identification and Tracking for Mining Automation*, Brisbane, Australia: CSIRO 2003

34 Einicke, G., Dekker, D, et al, *The survivability of underground communication systems following mine emergency incidents*, in 'Queensland Mining Industry Health and Safety Conference Proceedings 1997', New Farm (Australia): Queensland Mining Industry, ACCLAIM, p 217-222: 1997

35 Emslie, A.G.E.A., *Theory of the Propagation of UHF Radio Waves in Coal Mine Tunnels*, Pittsburgh PA USA: NIOSH 1975

36 EnGenius Inc, *Atheros 6thG Mini-PCI Adapter EMP-8602*, : 2009

37 Enste, U. and Müller, J, *Datenkommunikation in der Prozessindustrie : Darstellung und anwendungsorientierte Analyse*, München: Oldenbourg Verlag, ISBN 978-3-8356-3116-8, 2007

38 European Commission, *Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work*, Brussels: 1989

39 European Commission, *DIRECTIVE 2006/42/EC of 17 May 2006 on machinery*, Brussels: 2006

40 European Commission, *EMC Directive 2004/108 EC*, Brussels BE: 2004

41 European Commission, *EU ATEX Directive*, Brussels BE: 1994

42 European Commission, *EU Directive on Safety and Health of work equipment*, Brussels

BE: 2009

43 European Commission, *Eu Low Voltage Directive 2006/95EC*, Brussels, BE: 2006

44 European Commission, *EU Machine Directive: List of Harmonized Norms*, Brussels, Belgium: 2009

45 European Commission, *Guide to application of the Machinery Directive 2006/42/EC*, Brussels BE: 2010

46 Federal German Government, *Anforderungen an die Sicherheits- oder Gesundheitsschutzkennzeichnung (Mindestvorschriften)*, Berlin, Germany: 1995

47 Federal German Government, *Bergverordnung für für alle bergbaulichen Bereiche (Allgemeine Bundesbergverordnung - ABBergV*, Berlin, Germany: 1995 - 2009

48 Federal German Government, *Bundesberggesetz (BbergG)*, Berlin, Germany: 1980-2009

49 Furrer, *Industrieautomation mit Ethernet-TCP/IP und Web Technologie*, Heidelberg: Hüthig Verlag, ISBN 3-7785-2860-2, 2003

50 Gogolewska, A., *Surface and underground Mining Technology*, Wroclaw, Poland: Polytechnica Wroclawska, ISBN 978-83-62099-00-8, 2011

51 Harris, R., *Mine emergency communications: options, issues and status*, Charleston WV USA: West Virginia Office of Miners' Health Safety and Training 2007

52 Henniges, R., *Current Approaches of WiFi Positioning*, Berlin, Germany: TU Berlin 2012

53 Hoffmann, P., *ISBP1 Thermal Equivalent Test*, Ladbergen, Germany: MineTronics GmbH 2013

54 Huenefeld, R. and Mueller, C, *MineView – Mine Information and Monitoring for the Future*, in: 'Proceedings of the Conference for Applications of Computers and Operations Research in the Mining Industry', Magri, Santiago, Chile: 2007

55 Huenefeld, R., Küpper, T, et al, *ProNet 3D – Visualisierung markscheiderischer Daten im Intranet*, in: 'Tagungsband 44. Wissenschaftliche Tagung im Markscheidewesen', Deutscher Markscheider-Verein e.V, Bochum, Germany: 2004

56 Hürmann, T. and Giesselmann, T, *Automation and Communication in the Underground Logistics Area – Processes and Technology*, in: 'Proceedings of the 5th International Symposium High Performance Mining', Seeliger et al, Aachen: 2009

57 IAONA and ABB, *Industrial Ethernet: auf dem Weg zum Industriestandard - Volume D/E*, : Vogel Verlag, ISBN 3-8259-1910-2, 2001

58 IBExU GmbH, *ATEX Certificate MIC*, Freiberg, Germany: 2011

59 IBExU GmbH, *Prüfbericht IB-11-8-56 Gewährleistung des Explosionsschutzes von Lithium-Batterien*, Freiberg, Germany: 2011

60 IEEE Computer Society, *IEEE 802.1D Media Access Control (MAC) Bridges*, New York, USA: 2004

61 IEEE Computer Society, *IEEE 802.3-2002 Ethernet Standard*, New York, USA: 2002

62 International Electrotechnical Commission (IEC), *Functional safety of E/E/PE safety-*

related systems - Part 0: Functional safety and IEC 6150, Geneva, Switzerland: 2005

63 International Electrotechnical Commission (IEC), *Functional safety of E/E/PE safety-related systems - Part 1: General requirements*, Geneva, Switzerland: 1998

64 International Electrotechnical Commission (IEC), *Functional safety of E/E/PE safety-related systems – Part 2: Requirements for E/E/PE safety-related systems*, Geneva, Switzerland: 2000

65 International Electrotechnical Commission (IEC), *Functional safety of E/E/PE safety-related systems – Part 3: Software requirements*, Geneva, Switzerland: 1998

66 International Electrotechnical Commission (IEC), *Functional safety of E/E/PE safety-related systems – Part 4: Definitions and abbreviations*, Geneva, Switzerland: 1998

67 International Electrotechnical Commission (IEC), *Functional safety of E/E/PE safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*, Geneva, Switzerland: 1998

68 International Electrotechnical Commission (IEC), *Functional safety of E/E/PE safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*, Geneva, Switzerland: 2000

69 International Electrotechnical Commission (IEC), *Functional safety of E/E/PE safety-related systems – Part 7: Overview of techniques and measures*, Geneva, Switzerland: 2000

70 IREDES initiative, *International Rock Excavation Data Exchange Standard*, IREDES initiative, online available on: 22.5.2011 at www.iredes.org. Accessible in file: IREDESwhitePaper.pdf, 2010

71 ISEE S.L., *IGEP user manual*, Barcelona, Spain: 2010

72 Lagace, R L, et al, *PROPAGATION OF UHF RADIO WAVES IN LIMESTONE ROOM AND PILLAR MINES*, Cambridge, MA USA: NIOSH 1979

73 Landesoberbergamt NRW, *Brandschutztechnische Maßnahmen zur Errichtung und zum Betrieb von stationären Gurtförderanlagen mit Fördergurten in V-Qualität für Grubenbaue mit Wettergeschwindigkeiten > 3 m/s*, Arnsberg, Germany: 2001

74 Landesoberbergamt NRW, *Elektro-Bergverordnung Dritter Teil: Verwendung elektrischer Anlagen und elektrischer Betriebsmittel unter Tage*, Arnsberg, Germany: 2009

75 Landesoberbergamt NRW, *Energieversorgung und Warnung in Notsituationen*, Landesoberbergamt NRW, online available on: 30.12.2012 at http://esb.bezreg-arnsberg.nrw.de. Accessible in file: NRW-EnergieUndWarnung.pdf, 1990

76 Landesoberbergamt NRW, *Fluchtwegerichtlinie*, , online available on: 30.12.2012 at http://esb.bezreg-arnsberg.nrw.de. Accessible in file: NRW-RL-Fluchtwege.pdf, 1989

77 Landesoberbergamt NRW, *Rettungskonzept für den Steinkohlenbergbau unter Tage*, Arnsberg, Germany: 1993

78 Landesoberbergamt NRW, *Steuerungsrichtlinien*, Arnsberg, Germany: 1991/1996

79 Landesregierung NRW, *Bergverordnung Steinkohle*, Düsseldorf: Landesregierung NRW 1995

80 LINUX community, *DHCPD LINUX Manual Page*, , online available on: 28.5.2013 at http://linux.die.net/man/8/dhcpd. Accessible in file: DHCPD-Man.pdf, 2013

81 Linux Community, *iperf command Ubuntu Manual Page*, , online available on: 29.5.2013 at http://manpages.ubuntu.com/manpages/lucid/man1/iperf.1.html. Accessible in file: http://manpages.ubuntu.com/manpages/lucid/man1/iperf.1.html, 2013

82 Madsen, L., *Asterisk™: The Definitive Guide*, : O'Reilly Media Inc, ISBN 978-0-596-51734-2, 2011

83 Mahmoud, S.F., *Wireless Transmission in Tunnels*, in 'Mobile and Wireless Communications Physical Layer Development and Implementation', Rijeka, Croatia: Salma Ait Fares, InTech, p 2-24: 2010

84 Maptek Pty Ltd (Ed.), *3D Modelling and Mine Planning Software*, Brisbane Australia: Maptek Pty Ltd 2012

85 McKee, L., *OGC Standards and Cloud Computing*, : Open Geospatial Consortium 2011

86 Mikrotik SIA, *2.4/5GHz 802.11a+b+g High Power Wireless Mini-PCI Card*, Riga, Latvia: 2009

87 MineTronics GmbH, *All Center Servers Function Specification*, Ladbergen, Germany: 2011

88 MineTronics GmbH, *Device Specification MIC150*, Ladbergen, Germany: 2012

89 MineTronics GmbH, *ISBP1 - Technical description for ATEX certification*, Ladbergen, Germany: 2012

90 MineTronics GmbH, *MIC Technical Description for ATEX approval - Appendix 2*, Ladbergen, Germany: 2012

91 MineTronics GmbH, *MIC1 Mining Infrastructure Computer Device and System SOFTWARE User Manual*, Ladbergen, Germany: 2011

92 MineTronics GmbH, *MIC1, MMG1 Device Description for ATEX / IECEx approval*, Ladbergen, Germany: 2010

93 MineTronics GmbH, *MMG WLAN survey system User Manual*, Ladbergen, Germany: 2011

94 Minetronics GmbH, *MTP1 Loudspeaker test report*, Ladbergen, Germany: 2012

95 MineTronics GmbH, *MTP1 Underground Phone and Personal Communicator Specification*, Ladbergen, Germany: 2011

96 Minetronics GmbH, *Operating Instructions Battery Pack ISBP1*, Ladbergen, Germany: 2012

97 Minetronics GmbH, *Power Consumption MTP1 Test Report*, Ladbergen, Germany: 2012

98 MineTronics GmbH, *Safety related underground networks System Specification*, Ladbergen, Germany: 2009

99 Minetronics GmbH, *Switch module RSTP test report*, Ladbergen, Germany: 2011

100 MineTronics GmbH, *Technical Description for ATEX certification Device MTP1*, Ladbergen, Germany: 2012

101 MineTronics GmbH, *Underground Communication Network: NetCenter*, Ladbergen, Germany: 2012

102 MineTronics GmbH, *Universal Switch Module FSW2 Invitation to tender*, Ladbergen, Germany: 2010

103 MineTronics GmbH, *VoIP Center User Manual*, Ladbergen, Germany: 2012

104 MineTronics GmbH, *Wireless LAN Test OKD CSM Mine*, Ladbergen, Germany: 2012

105 MineTronics GmbH, *Wireless LAN Test Premogovnik Velenje Test Report*, Ladbergen, Germany: 2012

106 MineTronics GmbH, *WLAN Reichweitentests RAG Anthrazit Ibbenbüren*, Ladbergen, Germany: 2010

107 MineTronics GmbH, *WLAN throughput tests KWSA*, Ladbergen, Germany: 2012

108 MPL AG, *Magbes Switch Datasheet*, Baden, Switzerland: 2010

109 Mueller C, *Hardware Components for a Mining Infrastructure Computer for use in Safety related underground networks*, Ladbergen, Germany: 2009

110 Mueller, C., *Active network components for dynamic evacuation guidance in mines*, Ladbergen (Germany): MineTronics GmbH 2009

111 Mueller, C., *Advanced Communication Techniques: Ethernet and Wireless LAN for use in mining communications*, Ladbergen: 2009

112 Mueller, C., *Einheitliche, standardisierte Kommunikation zur Effizienzsteigerung von Bergwerken*, Glückauf, 142, (11): p 499, 2006

113 Mueller, C., *Improve Underground Safety with Higher Network Intelligence*, Engineering and Mining Journal, 214, (03): p 44-49, 2013

114 Mueller, C., *IREDES: Standardized integration of mining equipment into corporate IT infrastructures*, in: 'Proceedings of the 32nd APCOM Conference', S. Dessureault, Tucson, Az USA: 2005

115 Mueller, C., *Kommunikationsnetzwerk und Verfahren zur sicherheitsgerichteten Kommunikation in Tunnel- und Bergwerksstrukturen, Patent application PCT/EP 2010/056825*, Ladbergen: MineTronics GmbH 2010

116 Mueller, C., *MIC Mine Infrastructure Computer Platform Specification*, Ladbergen: MineTronics GmbH 2009

117 Mueller, C., *MTPhone Feature and Specification List*, Ladbergen: MineTronics GmbH 2011

118 Mueller, C. and Brenkley, D, *D1.2: Safety Assessment Methods for Mining Communication Systems*, : EMTECH project consortium 2010

119 Mueller, C. and Chen, G, *Safety related underground networks System Specification*, Ladbergen: MineTronics GmbH 2009

120 Mueller, C. and Noack, A, *EU RFCS EMTECH 3rd semester report - MineTronics part*, Ladbergen: MineTronics GmbH 2010

121 Mueller, C. and Noack, A, *EU RFCS EMTECH 4th semester report - MineTronics part*, Ladbergen: MineTronics GmbH 2010

122 Mueller, C. and Noack, A, *Safety Support Functions for Underground Network Communications*, in 'Proceedings of the 35th Application of Computers and Operations Research in the Minerals Industry Symposium 2011 (APCOM 2011) ', Wollongong, Australia: E. Baafi, Curran Associates Inc, p 827ff: 2011

123 Mueller, C., Noack, A, et al, *Mining Networks and the security question*, in '35th Application of Computers and Operations Research in the Minerals Industry Symposium 2011 (APCOM 2011) ', Wollongong, Australia: E. Baafi, Curran Associates, p 835-840: 2011

124 Mueller, C., Szekely, I, et al, *Emergency Switching and Network Functions for enhanced safety in underground networks*, in 'Proceedings of the 11th International Conference on DEVELOPMENT AND APPLICATION SYSTEMS, Suceava 2012', Suceava, Romania: Stefan cel Mare University of Suceava Faculty of Electrical Engineering and Computer Science, , p 103-106: 2012

125 Mueller, C., Szekely, I, et al, *Ethernet Communication for Detection of Emergency Locations and Dynamic Evacuation in Underground Infrastructures*, in 'Proceedings of the 12th OPTIM conference', Brasov (Romania): University of Transylvania, University of Transylvania, p : 2010

126 National Mining Association, *Mines Safety Handbook*, , online available on: 2008-12-06 at http://www.nma.org/pdf/010507_safety_handbook.pdf. Accessible in file: USA/NMA-MinesSafetyHandbook.pdf, 2006

127 net-snmp community, *snmpwalk Manual Page*, international: 2002

128 Niedersächsisches Oberbergamt, *Allgemeine Bergverordnung über Untertagebetriebe, Tagebaue und Salinen*, Clausthal-Zellerfeld: Niedersächsisches Oberbergamt 1966-1974

129 Niedersächsisches Oberbergamt, *Bergverordnung für die Erzbergwerke, Steinsalzbergwerke und für die Steine- und Erden-Betriebe (BVOESSE)*, Clausthal-Zellerfeld: Niedersächsisches Oberbergamt 2001

130 Noack, A., *Status Quo short analysis of safety related communications in underground coal mining*, Ladbergen: MineTronics GmbH 2011

131 OpenPicus, *Flyport Open Picus WiFi module*, : Eikon srl 2011

132 Oracle Corp., *Introduction to Java Platform, Enterprise Edition 6*, Redwood Shores, CA USA: 2010

133 Oxby, R., *Enhancing Safety Compliance and Improving Productivity with Integrated Communication System and Devices*, in 'Applications of Computers and Operations Research in the Mining Industry', Santiago (Chile): Magri, Gecamin Ltda, p : 2007

134 Panasonic Inc, *Datasheet Panasonic PSS cell 10446*, : Panasonic Inc 2010

135 Panasonic Inc, *Panasonic Lithium Ion Batteries*, : Panasonic Inc 2007

136 Papamichalis, A., *OPTIMINE RFCS project RFCS 2011-00001 Mid Term Report*, Ibbenbüren, Germany: 2013

137 Parlante, N., *Linked List Basics Stanford University*, Stanford: 2001

138 Platek, B., *Raport 22122012*, Wroclaw, Poland: Polytechnica Wroclawska 2012

139 Polytechnica Wroclawska, *MTP1 Thermal Test Report*, Wroclaw, Poland: 2012

140 Polytechnica Wroclawska, *RAPORT 05092012*, Wroclaw, Poland: 2012

141 Queensland Ombudsman (Publ.), *The Regulation of Mine Safety in Queensland*, Brisbane QLD Australia: Queensland Ombudsman 2008

142 Raimoaho, J., *Mine wide communication system*, in: 'Proceedings of the 4th regional APCOM', , Tampere, Finland: 2001

143 Sammarco, J.J., *Programmable Electronic Mining Systems: Best Practice Recommendations Part 1: 1.0 Introduction*, Cincinnati OH USA: U.S. National Institute of Safety and Health (NIOSH) 2001

144 Schiffbauer, W.H., *Coal Mine Communications Niosh Report*, Pittsburgh PA USA: NIOSH 2006

145 Sermersheim, J., *RFC4511: Lightweight Directory Access Protocol (LDAP): The Protocol*, Provo, Utah USA: 2006

146 SFF committee, *INF-8074i Specification for SFP (Small Formfactor Pluggable) Transceiver*, Santa Clara, CA USA: 2001

147 Siemens, *Open Transport Network (OTN)*, Olen, Belgium: 2013

148 Siemens, *OTN in Mining Applications*, , online available on: 2013-01-27 at http://www.otn.be/applications/mining. Accessible in file: OTN-Mining.pdf, 2013

149 SkeyeTek Inc, *RFID reader Module Data Sheet*, Westminster, Co USA: 2007

150 Slupski, P., *UPS Prototype Board testing - Test Report*, Ladbergen, Germany: MineTronics GmbH 2011

151 Smith, D. and Simpson, K, *Functional Safety: A Straightforward Guide to Applying IEC 61508 and Related Standards*, : Elsevier Butterworth-Heinemann, ISBN 0 7506 6269 7, 2004

152 Stallings, W., *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2, 3/E*, : Addison-Wesley, ISBN 9780201485349, 1999

153 Stevens, W., *TCP/IP Illustrated, Volume 1: The Protocols*, : Addison Wesley Publishing, ISBN 0-201-63346-9, 1994

154 Stevens, W., *UNIX Network Programming, Volume 1 Network API's*, Upper Saddle River: Prentice Hall, ISBN 0-13-490012-X, 1998

155 Sun, Z., *Channel Modeling and Analysis for Wireless Networks in Underground Mines and Road Tunnels*, IEEE Transactions on Communications, 58, (June): p 1758ff, 2010

156 Synder, D., *Communications and tracking research, Report and presentation to Mines Safety and Health Research Advisory Council (MSHRAC)*, Pittsburgh PA USA: 2007

157 Szabo, J., *Comunicaţii wireless în medii miniere în situaţii de urgenţă*, Targu Mures, Romania: 2011

158 Texas Instruments, *TPS 2421 Integrated FET Hot Swap Data Sheet*, Dallas, Tx USA: 2009

159 Texas Instruments, *VOLTAGE PROTECTION FOR 2-, 3-, OR 4-CELL Li-Ion BATTERIES (2nd-LEVEL PROTECTION)*, : 2008

160 Trounson, A., *Rio to trial automated mining*, The Australian, , (January): p , 2008

161 Ubiquity Networks Inc, *RouterStation CPU Module Spec*, Milpitas, CA USA: 2009

162 US Department of Labor - Mining Safety and Health Administration, *2010 Comparison of Year-to-Date and Total Fatalities for M/NM & Coal*, US Department of Labor - Mining Safety and Health Administration, online available on: at http://www.msha.gov/STATS/DAILY/d2010BAR.PDF. Accessible in file: MSHA/Fatalities2006-2010.pdf, 2010

163 USA Federal Government, *Mine Communications Technology Innovation Act*, USA Federal Government, online available on: 30.12.2012 at http://www.govtrack.us/congress/bill.xpd?bill=h110-3877 . Accessible in file: MCommTechInnovAct.pdf, 2007

164 USA Federal Legislation, *MINE IMPROVEMENT AND NEW EMERGENCY RESPONSE ACT OF 2006 (MINER ACT)*, Washington DC USA: Federal law doc No PL 109-236 (S2803) 2006

165 W3C and Droms, R, *RFC 2131: Dynamic Host Configuration Protocol (DHCP)*, 1997: 1997

166 W3C and Handley, M, *RFC 3261: Session Initiation Protocol (SIP)*, Berkley CA, USA:

167 Wacker Silicones, *RT602 Data Sheet*, München, Germany: 2009

168 Wacker Silicones, *Thixotropic Additive M and Stabilizer 43*, München, Germany: 2007

169 Wahl, M., *Authentication Methods for LDAP*, Austin, TX USA: 2000

170 Wigdén, I., *To install automation equipment in an underground mine*, in 'Proceedings of the 6th International Symposium on Mine Mechanization and Automation', Sandton, RSA: APCOM committee, , p 267ff: 2001

171 Wikipedia, *Leaky Feeder*, Wikipedia.org, online available on: 2013-01-27 at http://en.wikipedia.org/wiki/Leaky_feeder. Accessible in file: Wikipedia-LeakyFeeder.pdf, 2012

172 Wikipedia-Community, *Mining*, Wikipedia.org, online available on: 30.12.2012 at http://en.wikipedia.org/wiki/Mining. Accessible in file: WikipediaMining.pdf, 2012

173 Wikipedia-Society, *2010 Copiapó mining accident*, , online available on: 03.01.2013 at http://en.wikipedia.org/wiki/2010_Copiap%C3%B3_mining_accident. Accessible in file: WikiChile2010.pdf, 2013

174 Wolfert, P., *MAGBES Switch Power Cycle test*, Ladbergen, Germany: 2012

175 Wolfert, P., *MIC Power Consumption tests*, Ladbergen, Germany: 2010

176 Zeller, T., *OpenVPN kompakt*, Saarbrücken, Germany: Brain-Media, ISBN 978-3-939316-51-0, 2008

Page intentionally left blank

Curriculum Vitae

Personal information

Surname:	Mueller
First Name:	Christoph
Address:	Goethestrasse 50 49549 Ladbergen Germany
Phone:	+49 5485 830145
Cellphone:	+49 172 283 2717
Email:	chmueller@dm-technologies.com
Date of Birth:	1963-05-06
Place of birth:	Osnabrück / Germany
Nationality:	German

Professional Experience

2011 – present	Founder, shareholder and CEO of MT-Silesia Sp. z o.o. In Wroclaw / Poland, a company specialized on development of electronics hardware and industrial software
2009 – present	Founder, shareholder and CEO of MineTronics GmbH. A company specialized on electronics and networking in mining environments
2007 – 2009	Vice president Becker Mining Systems AG, Friedrichsthal, Germany responsible for Sales Scandinavia and for business development underground networking and IT portfolio
2007 – 2009	General Manager of Embigence GmbH
2002 – 2007	Owner and president of Embigence GmbH, a company focused on IT and communication systems for underground use.
1997 – 2002	Owner and president of DM Technologies GmbH&Co, a consulting company focused on automation, communication and IT design, architecture and project management for underground machines and mining operations.
1992 – 1997	Group leader for mining machine automation in the mining R&D division of the E. Heitkamp GmbH Herne. Development of IT components for advanced and IT based machine control systems.

1990 – 1992	After three months appointed group leader for UNIX systems of the Heitkamp group. During this time e.g. responsible for the successful integration of PC workstations and setup of an Ethernet based network at the headquarters.
1990	System support group member servicing UNIX and PC systems in the E. Heitkamp GmbH, Herne:

Professional Training

2008	Management training (Malik Management St. Gallen, Switzerland)

Education

1969 – 1972	Elementary School, Liebfrauengrundschule Osnabrück
1972 – 1979	Gymnasium Vinzenz Pallotti Kolleg, Rheinbach bei Bonn
1980 – 1982	Kardinal von Galen Gymnasium, Mettingen/Westf Exam: Abitur
1982 – 1987	Diploma Studies of Agricultural Engineering with Fachhochschule Osnabrück incl. practical semesters and postgraduate extension of diploma works on electronics for agricultural machines
1989 – 1990	Studies of Technical Software Engineering at Siemens AG

Languages

German:	Excellent (mother tongue)
English:	very good written and oral skills (Negotiation level)
Norwegian:	good written and oral skills (Negotiation level)
Swedish:	good written and oral skills (Negotiation level)
Dutch:	passive (understanding and reading)

Working Experience and Expertise

1986 - 1987	Development of a modular on board computing unit for agricultural machines (Diploma thesis); After Diploma thesis application on different machines (Combines, harvesters)
1984 – 1989	Development of a invoicing software for agricultural machine services (successful in use until 1996) on Apple IIe computer
1985	Development of a linear optimization software for feed ingredient

	optimization at lowest cost on Apple IIe computer
1992 – 1993	Consulting for the interface between passenger area and the ship's technical installations for newbuilding of the Norwegian coastal steamer M/S Richard With for OVDS ASA, Narvik, Norway
1997	Design Study for new, software based functions and products for mining machines (Atlas Copco, Stockholm, Sweden)
1997 – 2000	Project management for the worlds first fully commercial autonomous drill rig project with up to 6 unmanned drill rigs operated from a central control room in the iron ore mines of LKAB, Sweden. The project covered the introduction of new production level, new machines, new control systems and new wireless digital communications.
2000 – 2001	Design of a generic remote control concept for mining machines including demonstrator implementations (Atlas Copco Rock Drills AB, Örebro, Sweden)
2000 – recent	Chairman of the International Rock Excavation Data Exchange Standard, an industry initiative that standardizes information exchange between mining machines and central computer systems.
2003	Embigence performs first wireless LAN implementations for underground machines
2006	Embigence pioneers the WLAN use in underground coal mining by supplying over 200 accesspoints to Deutsche Steinkohle AG
2006	Embigence successfully and fully commercially implements the world's first longwall shearer communicating via WLAN
2004 – 2007	Embigence implements a fully autonomous (unmanned) monorail system for underground use.
2005 – 2007	Embigence implements a WLAN communication and an integrated digital video system with seamless roaming for Atlas Copco loaders.
2009 - present	MineTronics implements a new underground network communication system enabling the use as safety support system; Development supported by the EU Research Fund for Coal and Steel (RFCS) within the EMTECH project.
2010 – present	Responsible for the functional description and automation of a new mechancial rock excavation machine as a joint project of Atlas Copco and Rio Tinto

Awards

2007	Innovation award of „Deutsche Steinkohle AG“ for an autonomous monorail system

Scientific Conference activities

2001	ISMMA conference: Session chairman
2002	CIM conference: Session chairman
2005	APCOM 2005 conference: Member of the International Committee incl. paper review, Session chairman
2007	APCOM 2007 conference: Member of the International Committee incl. paper review, Session chairman
2008	MassMin2008 conference: Member of the International Committee incl paper review, Session chairman
2008	MinIn 2008 conference: Member of the technical committee and paper review
2009	APCOM 2009 conference: Member of the International Committee incl. paper review, Session chairman
2011	APCOM 2011 conference: Member of the International Committee incl. paper review, Session chairman
2012	MassMin 2012 conference: Member of the International Committee incl paper review

Publications – General: 35 publications

1	Conference Key Note
25	Conference Papers
7	Articles
1	Editorial
1	Chapter in Book

Publications – PhD Thesis specific: 7 publications

5	Conference Papers
1	Conference paper published in Thomson-Reuters (ISI) Conference Proceedings Indexed conference (OPTIM 2010)
1	Thomson-Reuters (ISI) indexed journal article: Mueller, C., „*Improve Underground Safety with Higher Network Intelligence*“, Engineering and Mining Journal, 214, (03): p 44-49, 2013

Glossary

ATEX	French "*Atmosphère explosible*", Synonym for the explosion protection directive 94/9 EU of the European Commission.
BPDU	Bridge Protocol Data Unit: Administrative telegram used by the IEEE802.1D Real Time Spanning Tree Protocol (RSTP) used to exchange STP/RSTP information between the bridges.
CAD	Computer Aided Design
Center Node	*MIC* in the logical "center" of an isolated underground network which is the master node in handling the *Emergency Mode*.
Central System	IT systems to configure and operate the underground network, store tracking records of people and assets underground and to enable network based voice and data communication to devices underground when the network operates in regular mode (Chapter 2.5)
CPU	Central Processing Unit
CSMA/CD	Carrier sense multiple access with collision detection
Diameter:	The network diameter is the maximum eccentricity of all nodes (vertices) of the network (graph).
DHCP	Dynamic Host Configuration Protocol
Eccentricity:	The eccentricity is the maximum distance between two nodes of a given network. Therefore, each node has its own eccentricity value. A node with a low eccentricity is usually located more close to the center of the network whereas nodes on the outside of the network are having higher eccentricity values.
EEPROM	Electrically Erasable Programmable Read-Only Memory
EMC	Electromagnetic Compatibility
Emergency Application	Applications running on the *MIC*s, activated by the *Emergency Mode*. These applications help the people underground in gathering them in one place, guiding them on possible evacuation pathes etc.
Emergency Mode	Operation Mode of the *MIC* in which the connections to

	above ground are lost and the underground network independently supports the people under ground in handling the emergency situation by running *Emergency Applications*, gathering people in one place, guiding them on possible evacuation pathes etc.
Field Application Systems	Emergency handling applications running on personal devices (Smartphones or PDA's), on network nodes or as separate stationary network devices in order to help miners to deal with the emergency situation.
Functional Module	Electronics module in a steel enclosure providing specific functionality within a MIC System.
GML	Geography Markup Language, XML based data structure definitions for geographic features
IREDES	International Rock Excavation Data Exchange Standard. Open, XML schema based standard for field device information exchange in the mining industry
JTAG	Joint Test Action Group
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MAC	Media Access Control address
MIC	"*Mining Infrastructure Computer*", Network node consisting of an application CPU, (fiber optic) managed switch(es), WLAN accesspoint(s) and optional peripherals used as an universal underground networking device, safety support unit and mining infrastructure application computer.
MEMS	Micro Electro Mechanical Systems
MIC System	Composition of MIC Modules in one electrically connected installation underground.
MMG	Mobile Machine Gateway
MSHA	Mine Safety and Health Administration (Agency of the United States department of Labor)
MTBF	Mean Time Between Failure

NetCenter	Central server software to upload software and configurations to underground networking devices and to acquire and process status information from those devices.
NIOSH	National Institute of Operational Safety and Health (USA)
Normal Mode	Also: *Normal Operation Mode.* This is the operation mode the system runs in when there is no active emergency (Emergency Mode not active)
NTP	Network Time Protocol
PBX	Private Branch Exchange
PCB	Printed Circuit Board
PCB-A	Assembled Circuit Board
PCI	Peripheral Component Interconnect. Specifies the bus interface for peripheral devices in personal computers
PDA	Personal Digital Assistant
PFD	"*Probability of Failure on Demand*". Defines the maximum probability of a dangerous failure in a Safety Integrity Level defined system [67].
RAM	Random Access Memory
RF	Radio Frequency
RFID	Radio Frequency ID
RSTP	Real Time Spanning Tree Protocol, Method in accordance to IEEE802.1D to assure a loop free Ethernet network in ring or mesh topologies.
SIL	Safety Integrity Level; Relative level of risk reduction or a target level of risk reduction used for safety relevant functions. Specified in EN 61508 [67]
SAR	Search-And-Rescue
SafeCenter	Above ground server which stores all static safety information for download to the underground *MICs*. The server also is part of the *Topology Application* in order to have an overview of the momentary underground network situation. Furthermore it handles an *Emergency Mode* in the safety center above ground. It is also used for system configuration as e.g. test and training mode configurations.

Safety Support Network	Underground network installation consisting of intelligent network nodes (like the *MIC*) to support underground workers handling emergency situations in a controlled way and to support fast and goal oriented rescue while reducing time needed for search operations.
SCADA	"Supervisory Control And Data Acquisition", Supervision and Control of technical processes using computer systems
SFP	Small Form factor Pluggable. Fiber optic transceiver modules following a specific standard for electromechanic layout and data exchange [146] in order to allow different fiber optic phsical standards to be connected to one single network switch
SIL	Safety Integrity Level
SIP	Session Initiation Protocol in VoIp telephony
SMS	Short Message Service
SNMP	Simple Network Management Protocol
STA:	Spanning Tree Algorithm (can be either STP according to 802.1D < 2004 or RSTP according to 802.1D >= 2004).
Status Telegram	Telegrams exchanged within a Multicast-Group between the *MICs* among each other and the *NetCenter* server in order to communicate the real time network layout and status. Via the *Status Telegram* also the *CenterNode* request and status information is exchanged.
TCP/IP	Transmission Control Protocol / Internet Protocol
TFT	Thin-Film Transistor technology for liquid crystal displays
TLV	"*Type Length Value*", Method for specifying content in a data communication protocol with Type specifying the data type, Length to specify the length of the Value field, while Type and Length are fixed length fields and Value is a variable length as specified in the Length field.
TrackCenter	Central server software to store the locations of people and assets underground on an above ground IT system.
Topology Application	Application running on the *MIC* and on a central server used to determine the current status of the other *MIC*s and the interconnecting network links.
UDP	User Datagram Protocol

UPS	Uninterruptable Power Supply, battery power supply which provides electrical energy to the devices in case the mains power drops.
USB	Universal Serial Bus
VLAN	Virtual LAN
VoIP	Voice over Internet Protocol
VoIPCenter	Central server software to organize VoIP audio channels. Consists of a standard SIP server and a web based user interface to conveniently group participants and to switch loudspeaker lines and telephones
VPN	Virtual Private Network
WLAN	Wireless LAN
XML	Extensible Markup Language

Pictures

Figures

Page intentionally left blank

7 APPENDICES

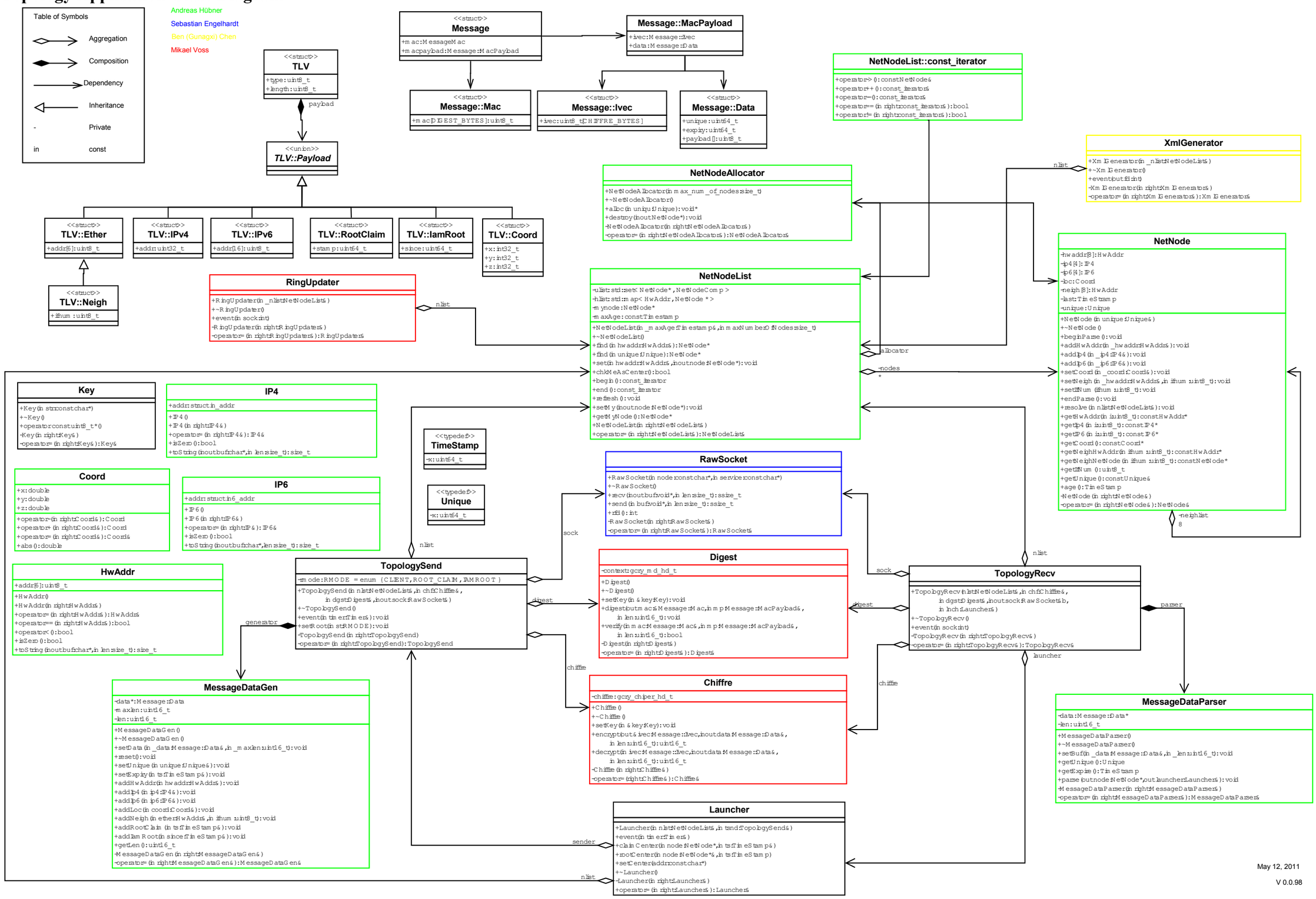
APPENDIX 1: XML Generator: XML schema

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://www.minetronics.com/EMTECH/topology/xml">
   <xs:annotation>
      <xs:documentation>
         This schema is created for EMTECH project for the topology application.
         All network device nodes have to follow this schema to create the
topology XML.
      </xs:documentation>
   </xs:annotation>
   <xs:element name="NodeList">
      <xs:complexType>
         <xs:sequence>
            <xs:element name="Node" type="NetNode"
maxOccurs="unbounded"/>
         </xs:sequence>
      </xs:complexType>
   </xs:element>
   <xs:complexType name="NetNode">
      <xs:sequence>
         <xs:element name="id" type="Unique">
            <xs:annotation>
               <xs:documentation>
                  A unique id of a MIC (64 bit unsigned int)
               </xs:documentation>
            </xs:annotation>
         </xs:element>
         <xs:element name="ipv4" type="IPv4" minOccurs="0"
maxOccurs="unbounded">
            <xs:annotation>
               <xs:documentation>
                  IP address version 4 of MIC. A MIC could have 0 or more ipv4
addresses.
               </xs:documentation>
            </xs:annotation>
         </xs:element>
         <xs:element name="ipv6" type="xs:string" minOccurs="0"
maxOccurs="unbounded">
            <xs:annotation>
               <xs:documentation>
                  IP address version 6 of MIC. A MIC could have 0 or more ipv6
addresses.
               </xs:documentation>
            </xs:annotation>
         </xs:element>
         <xs:element name="hwAddr" type="xs:string" minOccurs="0"
maxOccurs="unbounded">
            <xs:annotation>
               <xs:documentation>
                  Hardware address of MIC. A MIC could have 0 or more hardware
addresses.
               </xs:documentation>
            </xs:annotation>
         </xs:element>
         <xs:element name="nInterfaces" type="xs:integer">
```

```
            <xs:annotation>
               <xs:documentation>
                  Number of network interfaces of MIC. This property is used to
trace all neighbor devices (MICs).
                  For one MIC, there could be one or more interfaces. Each interface
is associated with zero or one neighbor device.
               </xs:documentation>
            </xs:annotation>
         </xs:element>
         <xs:element name="location" type="Coord">
            <xs:annotation>
               <xs:documentation>
                  MIC geographical location. This is a coordinate in the mine.
                  This parameter must be set at MIC installation.
               </xs:documentation>
            </xs:annotation>
         </xs:element>
         <xs:element name="age" type="xs:dateTime">
            <xs:annotation>
               <xs:documentation>
                  Time since last update.
               </xs:documentation>
            </xs:annotation>
         </xs:element>
         <xs:element name="Neighbors">
            <xs:annotation>
               <xs:documentation>
                  This is a list of all neighbors of this MIC.
                  Each of the these neighbors is related to one interface, one unique
id of the device and it's hardware address.
               </xs:documentation>
            </xs:annotation>
            <xs:complexType>
               <xs:sequence>
                  <xs:element name="neighbor" minOccurs="0"
maxOccurs="unbounded" type="NeighborType"/>
               </xs:sequence>
            </xs:complexType>
         </xs:element>
      </xs:sequence>
   </xs:complexType>

   <xs:complexType name="Coord">
      <xs:sequence>
         <xs:element name="x" type="xs:decimal"/>
         <xs:element name="y" type="xs:decimal"/>
         <xs:element name="z" type="xs:decimal"/>
      </xs:sequence>
   </xs:complexType>

   <xs:complexType name="NeighborType">
      <xs:sequence>
         <xs:element name="interface" type="xs:string"/>
         <xs:element name="neighborId" type="Unique"/>
         <xs:element name="neighborHwAddr" type="xs:string"/>
      </xs:sequence>
   </xs:complexType>
```

```
    <xs:simpleType name="Unique">
      <xs:restriction base="xs:string">
        <xs:minLength value="64"/>
        <xs:maxLength value="64"/>
      </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="IPv4">
      <xs:restriction base="xs:string">
        <xs:maxLength value="15"/>
        <xs:maxLength value="7"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:schema>
```

APPENDIX 2: Topology Application Class Diagram



From: [8]

DECLARAŢIE

Subsemnaţii: MÜLLER Christoph

(nume şi prenume doctorand)

în calitate de student - doctorand al IOSUD:

Universitatea “Transilvania” din Braşov

(denumire IOSUD)

autor al tezei de doctorat cu titlul: **Applicability of Wired and Wireless Ethernet Networking Systems as Unified Safety Relevant Communication System in Underground Mines (editată în limba engleză) – Aplicabilitatea sistemelor de reţele Ethernet cablate şi wireless ca sisteme de comunicaţii de siguranţă relevante în mine subterane (RO)**

(titlul tezei de doctorat)

şi

Prof.dr.ing. SZEKELY Iuliu

(nume si prenume conducător doctorat)

în calitate de Conducător de doctorat al autorului tezei

la instituţia Universitatea “Transilvania” din Braşov

(denumire institutie)

declarăm pe proprie răspundere că am luat la cunoştinţă de prevederile art.143 alin (4) si (5)* şi art. 170** din Legea educaţiei naţionale nr.1/2011 şi ale art. 65, alin.5 – 7***, art. 66, alin (2)**** din Hotărârea Guvernului nr.681/2011 privind aprobarea Codului Studiilor universitare de doctorat şi ne asumăm consecinţele nerespectării acestora.

Semnătură	Semnătură
Student doctorand	Conducător de doctorat

((4)indrumatorii lucrărilor de licenţă, de diplomă, de disertaţie, de doctorat răspund solidar cu autorii acestora de asigurarea originalităţii conţinutului acestora

(5) este interzisă comercializarea de lucrări şptiinţifice în vederea facilitării falsificării de către cumpărător a calităţii de autor al unei lucrări de licenţă, de diplomă, de disertaţie sau de doctorat.

** **(1)**În cazul nerespectării standardelor de calitate sau de etică profesională, Ministerul Educaţiei, Cercetării, Tineretului şi Sportului, pe baza unor rapoarte externe de evaluare, întocmite, după caz, de CNATDCU, de CNCS, de Consiliul de etică şi management universitar sau de Consiliul Naţional de Etică a Cercetării Ştiinţifice, Dezvoltării Tehnologice şi Inovării, poate lua următoarele măsuri, alternativ sau simultan:

- **a)** retragerea calităţii de conducător de doctorat;
- **b)** retragerea titlului de doctor;
- **c)** retragerea acreditării şcolii doctorale, ceea ce implică retragerea dreptului şcolii doctorale de a organiza concurs de admitere pentru selectarea de noi studenţi-doctoranzi.

(2) Reacreditarea şcolii doctorale se poate obţine după cel puţin 5 ani de la pierderea acestei calităţi, numai în urma reluării procesului de acreditare, conform art. 158.

(3) Redobândirea calităţii de conducător de doctorat se poate obţine după cel puţin 5 ani de la pierderea acestei calităţi, la propunerea IOSUD, pe baza unui raport de evaluare internă, ale cărui aprecieri sunt validate printr-o evaluare externă efectuată de CNATDCU. Rezultatele pozitive ale acestor proceduri sunt condiţii necesare pentru aprobare din partea Ministerului Educaţiei, Cercetării, Tineretului şi Sportului.

(4) Conducătorii de doctorat sunt evaluaţi o dată la 5 ani. Procedurile de evaluare sunt stabilite de Ministerul Educaţiei, Cercetării, Tineretului şi Sportului, la propunerea CNATDCU.

***(5) teza de doctorat este o lucrare originală, fiind obligatorie mentionarea sursei pentru orice material preluat.

(6) studentul - doctorand este autorul tezei de doctorat şi îşi asumă corectitudinea datelor şi informaţiilor prezentate în teză, precum şi a opiniilor şi demonstraţiilor exprimate în teză

(7) conducătorul de doctorat răspunde împreună cu autorul tezei de respectarea standardelor de calitate sau de etica profesională, inclusiv de asigurarea originalităţii conţinutului, conform art. 170 din Legea nr. 1/2011.

**** protecţia drepturilor de proprietate intelectuală asupra tezei de doctorat se asigură în conformitate cu prevederile legii.