Emergency Switching and Network Functions for enhanced safety in underground networks

Christoph MÜLLER[1], Iuliu SZEKELY[2], Andreas HÜBNER[1]
[1]*MineTronics GmbH, Germany*
[2]*Sapientia University, Faculty of Technical and Human Sciences, Tg. Mures, Romania*
cmueller@minetronics.com, gszekely@ms.sapientia.ro, ahuebner@minetronics.com

***Abstract* — Location based services become more and more common in daily life: People and devices can be tracked permanently in a network. However, an Ethernet network – and its applications – always needs central services to work. Networks carrying safety information in areas where the network structure is exposed to natural damage like in underground mines therefore need special setups and applications in order to fulfill their purpose even in emergency cases, when communication is of special importance.**

Within a recent development project the use of network immanent information for the purpose of supporting safety of workers was implemented. This includes Emergency Mode Switching and location based services, even when all contact to central systems is lost. The related network level algorithms are subject of this paper. It describes how all network nodes make use of network internal status and traffic information to individually detect whether the overall network runs in regular mode or whether a transition into an Emergency mode is required in order to keep local communication under ground functional. Besides presenting the methods, the paper also reports on the tests carried out in order to verify the developments performed. The extraction and application level use of network immanent status information for location based services and the related methods are not exclusive to mining applications and can be of generic interest also for applications in other industries.

***Index Terms* — network, switching, underground network, emergency, mining applications**

I. INTRODUCTION

In traditional underground mining operations, most communication is carried out via telephone systems and analog radio communication. These systems all lack of redundancy and availability in the case of major emergencies [1]. This lack of availability mainly originates from the fact that these systems are operating on single ended cabling in star like setups. The consequence from this setup is that the cutting of a trunk line which may be caused by a major mining emergency as e.g. a fire, an explosion or rock fall leads to a complete blackout of any communication in the affected area. In respect of international regulations and best practice rules for occupational safety and health as well as for functional safety of safety relevant installations this status can be regarded insufficient [1]. Already prior to the mining accident in Chile these facts were the background for the EU Commission to grant funding for a development project for emergency support systems which also included using a network based communication system as highly resilient method for communication and to use this network to provide location based services to the miners in case of an emergency [1] [2].

This includes four basic ideas [1]:

1. The network should have increased availability beyond the conventional ring redundancy.
2. The underground network shall stay alive in case of an emergency without the need of an online connection to any central server system.
3. The underground network shall collect, process and distribute the location of workers (“tracking”) independently from access to central systems
4. The underground network shall use tracking data, network status and environmental information to support potentially trapped workers in self rescue as well as support search and rescue teams in finding people.

This paper concentrates on the processes used for keeping the network alive when communication to central systems is lost (“Emergency Mode Switching”) and the related network mode switching operations.

II. THE UNDERGROUND NETWORK

Beyond the (still mandatory) telephone system most communication in modern mines is carried out using Ethernet infrastructures [3][11]. Due to the cable length needed this is preferably set up using fiber optic cabling. This applies even to underground coal mining where explosive gases (methane) may conform a potentially hazardous environment [3]. For redundancy reasons the network preferably is set up in ring structures where each ring is routed to above ground via two different shafts [3] [11].

The active components (“Network Nodes”) conform of managed switches, daisy chained in a ring structure. At these switches branch lines are connected to distribute the network into the underground workings. Thereby, the network can be setup to perfectly follow the tunnel infrastructure layout. In order to enable the Network Nodes to provide safety related location based functions, the layout of the network in relation to the tunnel infrastructure has to be known. As it cannot be predetermined where an emergency will occur, this knowledge has to be available in each single Network Node.

Rather than being a pure network switching unit, the Network Node now performs mining safety related application functions. This is the reason for calling these nodes “Mining Infrastructure Computer (MIC)”. Such computer generally consists of an application CPU, one or more managed fiber switch(es) and up to two WLAN accesspoints [4].

On each MIC a vector – node model of the mine's tunnel layout is stored, which conforms the basis for all location based functions. This model is downloaded from central servers during device startup and updated during regular operation. It contains the positions of the tunnel crossings as nodes and the distance of the tunnel segments between crossings. This pure tunnel infrastructure model is extended by the positions of safety-related elements like emergency exits, shelters, firefighting equipment etc. which are given a position in relation to the infrastructure model.

As an overlay to the tunnel infrastructure model, a model of the network infrastructure with the positions of all Network Nodes (MICs) as well as their interconnections is downloaded to the MICs. This enables the network to link network originated information (like the position of a miner acquired via the WLAN by one MIC) to the true position in the mine as defined by the underlying tunnel infrastructure model. The network infrastructure model is then assigned online status information like “link available” or “link down” which is generated online by all MICs. This procedure is performed using a so called “Topology Application” running on each MIC.

III. Network Setup Preconditions

In order to provide the safety-related functions, the network setup has to meet a number of preconditions. A typical network layout is shown in figure 1 [5]. This presumes that all MICs together with the NetCenter and other Center servers potentially required have to reside within one single collision domain.

Virtual Lans (VLANs) may be used throughout the network however it is recommended that all network administrative and safety-related functions (incl VoIP audio) are running in the untagged (non-VLAN) network in order to minimize the potential of functional problems during regular operation and Emergency mode switch-over.

In regular operation (“Normal Mode”), the IP addresses are assigned via a central system above ground. In case of an emergency, this system however has to be regarded inaccessible, which requires the underground network nodes to assign IP addresses independently. In order to prevent from IP address collisions when the networks re-connects to the central Dynamic Host Configuration Protocol (DHCP) server, the Network Nodes in Emergency Mode preferably uses a different range of IP addresses than the above ground DHCP server.

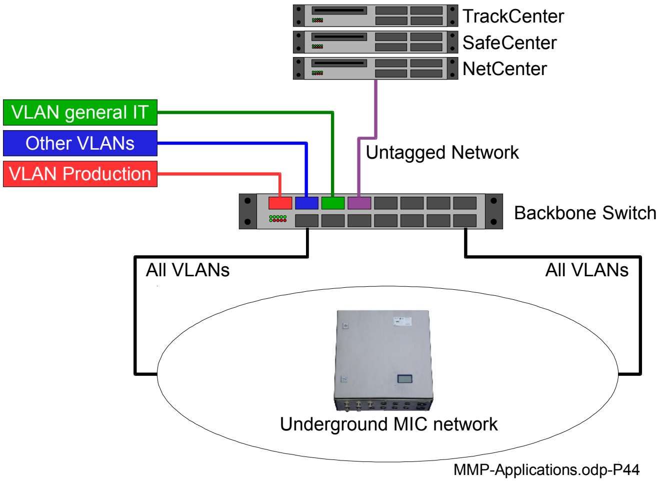

Figure 1: Virtual LANs and Central Systems

As during an emergency multiple isolated networks may be created, each independent island may use a different range of IP addresses which e.g. originates on the own (static) IP address of the network node acting as DHCP server. This minimizes the risk for collisions when the networks join and provides a maximum of operational reliability. As special operational condition it has to be assured that all such network functions and the related applications have to be tested as well as people have to be trained in using the safety support functionality. This is especially difficult as such tests and trainings have to be performed in networks which during test and training have to be used for full mining production. Therefore, it is recommended that all production relevant networks should use separate Virtual LANs. This enables to switch the untagged LAN to Emergency Mode while all other functions still remain active as needed in regular operation. However, the only function affected is the VoIP voice communication as this function is part of the (untagged) safety network. To ensure that operational voice messages are communicated even during tests and trainings, it has to be assured that the above ground dispatcher always is part of the voice communication group (which is needed for the training nevertheless). This means that for test and training purposes, the network island will be created by logically cutting the links at the MICs leaving a channel open for connecting the dispatcher to the VoIP communication group.

IV. Network Topology Determination

The MIC network nodes consists of an application CPU and a managed switch. The MICs exchange administrative messages among each other. These messages are using encryption routines to assure origin and authenticity of the messages exchanged. The connected switches determine the neighbors on each connected port by using a script containing the (insecure) snmp “*snmpwalk*” [12] command which determines the MAC of the device directly connected to this port. In a complex infrastructure this in turn also will be a switch which in an underground network is embedded into another MIC.

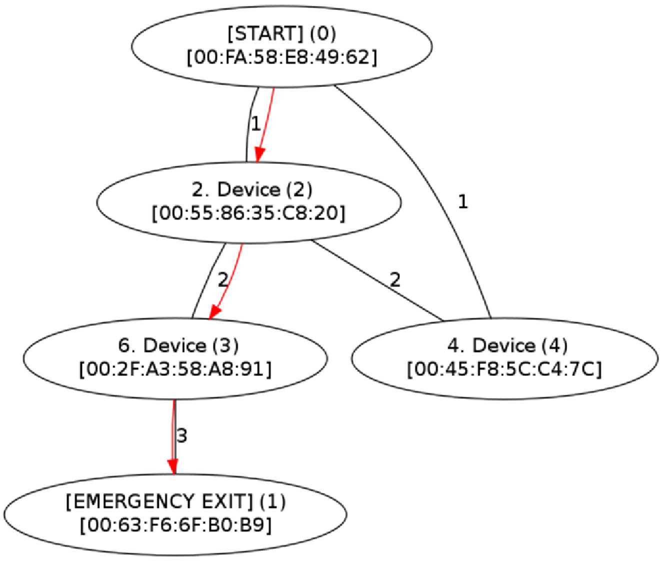

Figure 2: Simple Network Topology Graph

To avoid problems related to a sole use of snmpwalk to detect the network structure [12] and to assure a secured communication of the topology information between the MICs, the result of the *snmpwalk* query is distributed via a secured communication of topology messages sent between the MICs. These messages contain the results of all queries for each port of the assigned switches together with the tables of their corresponding neighbors. This results in a complete topology tree available to every MIC as shown in the simplified example in picture 2. By this data each MIC is able to evaluate the real time network structure of the network within its Ethernet collision domain.

This network topology graph is an important basis in order to start up and to handle the Emergency Mode.

V. Redundancy Connections

Before the network switches to Emergency Mode, it tries to find a redundant connection to the above ground systems to keep the regular operation running.

Redundancy connections in such ring- or mesh structures are handled by the Real Time Spanning Tree (RSTP) protocol in accordance to IEEE 802.1D-2004 [7]. To provide additional network resilience, not only rings are used but also entirely meshed structures. However, these structures are limited in size by the RSTP standard:

In IEEE 802.1D-2004 RSTP, the number of hops for the RSTP evaluation message ("BPDU") is limited in the "MaxAge" parameter to a value of 20 by default and up to 40 as a maximum. If this parameter value is exceeded, the BPDU is not going to be processed by the receiving switch. In such case, multiple Root Bridges will be randomly created which results in the computation of multiple Spanning Trees that are not able to exchange any information. [7]. As this is a crucial limitation for the entire system, related tests were carried out resulting in the conclusion that the network diameter must not exceed the "Max Age" setting of RSTP and all switches have to operate on the same setting of "Max age". Changing the parameter from the default of 20 to the maximum of 40 is not recommended due to potential side effects which may require tweaking of other parameters [8]. As a direct consequence and to assure full standard compliance the application networks have to be designed so the parameter can be met by assuring that the max number of hops from any point to any other does not exceed the related setting[5]. This fact was confirmed in a number of laboratory scale tests carried out with up to 20 managed switches in rings and meshed structures.

An alternative for the future would be to use non standardized and proprietary routines which are not exposed to these limitations if the applications demand that. For this, the logic tree available in each MIC together with proprietary functions in the switch hardware can be used as an algorithmic basis.

VI. Switching to Emergency Mode

The Emergency Mode is defined by the fact that all network communication to above ground central systems is lost and this communication cannot be reestablished within a certain amount of time by the RSTP functions using alternative paths.

Entering into Emergency Mode is performed by each MIC individually. It requires that the status messages between MIC and the central NetCenter server are not received any longer for a minimum amount of time.

Loosing contact to the central systems also means that central network services like DHCP and SIP are not available any longer. Therefore, the first action after detecting the contact loss is to assure that the disconnected part of the network arranges the availability of such central services. As a precondition, the MICs inside the isolated network "island" have to find a way of determining how to provide these central functions:

In a first step, the central node of the network island has to be determined. This is the node with the least amount of hops to all endpoints of the functional network. This point most probably at the same time also can be regarded the most safest place. For this purpose, every node determines the number of intermediate nodes from his own position to all endpoints of the network where an endpoint is defined as a node which only has one single connection to the network. This results in a number of paths to reach each endpoint of the network with each path having a number of hops to reach each endpoint of the network. This number is broadcast over the network by each node, so all nodes can compare the incoming results with their own result.

After all nodes have reported their numbers on the network, the center node is defined as being the node which reaches all endpoints with the minimum and most equal number of hops for every path. This is the node which has the lowest variance on the hop counts for every single path.

This fact is detected by every node independently after the node count reporting packets from all nodes have been received. After expiry of an additional waiting time the node which broadcast the least hop count is starting the Center Node functionality for the network island.

In case two nodes report the same number of hops to all endpoints, the first issuing the number is going to be the new Center Node. During the hop count investigation only active links are taken into account whereby standby redundancy connections are not counted thus providing circular counts to occur. Tests have been carried out on this algorithm showing that the algorithm works well and reliably. However tests showed that a number of special situations have to be taken into account which have to be handled separately [9]:

1. Two formerly isolated networks joining together e.g. when somebody repairs a broken link which not only results in two center nodes available in the network but also to potentially double assigned DHCP addresses for clients.
2. A networks splits off into two separate networks which will be the case when e.g. a node runs out of battery power or a link breaks.
3. Two nodes fully simultaneously assign themselves as center nodes (which is equal to parts of case No. 1)

The case of two isolated networks joining each other is solved in the way that the bigger network central services also take control over the smaller part. The central services of the smaller part are discontinued. An alternative in this case is using the algorithm as defined for two nodes assigning themselves as center simultaneously (case 3): In this case, the node with the higher MAC address wins and takes over the central node function.

The case of the network island splitting off in two or more separated islands is handled by the same routines as when an underground network initially looses contact to the regular central systems.

Once assigned, the new center node provides DHCP functions and determines which of his neighbors will have to provide the Session Initiation Protocol (SIP) [13] service for VoIP audio communication. The audio communication in emergency mode is set to conference mode where the loudspeakers of all units propagate all information talked in the network. This requires discipline during voice communication however it assures that all people in the area instantly get access to all information exchanged among them. During Emergency Mode all MICs regard the center node as the new "NetCenter" meaning that they also perform the status message exchange in case the network is split up further so that a recursive generation of emergency network cells can be assured.

During Emergency mode also all other safety support functions are provided like emergency exit guidance, assuring that nobody is left behind etc. [2].

VII. Recovery to Regular Operation Mode

Recovery to Regular Operation Mode is initiated when the center node of a network is able to reach the above ground NetCenter again for a continuous period of some minutes. For a clean recovery to Regular Operation Mode it is required that the DHCP addresses for network clients in Emergency Mode are assigned in the same collision domain like in the Regular Operation Mode. When the network then links up with the center again, no re-assignment is required. Before the Emergency mode is terminated, all client devices are informed that Emergency Mode will be finished soon. This can be performed either by text messages on displays and by playing an audio file from disk which tells to all VoIP participants that the switch over to regular operation will be performed shortly.

During this time, the central services on the emergency mode Center Node will terminate in order to let the central systems take over again.

IV. Conclusions And Future Work

The development work carried out demonstrates an "intelligent" underground network consisting of application programmable CPU's together with managed switches in every distributed network node. Every node CPU creates an own, independent real time network topology overview used for safety support features as an overlay to the geographic tunnel infrastructure. The setup of the tunnel infrastructure view is performed using standard Simple Network Management Protocol (SNMP) features together with application level network protocols for the exchange of topology information as well as application level safety support information.

The topology information is the basis for giving support to the people underground in case of an emergency as it is used for guidance to exits, shelters etc as a kind of electronic "underground navigation system". A precondition for this is that the nodes detect the presence of an emergency situation which is the case, when all connections to above ground servers are cut and therefore no access to central servers is possible. This fact is detected by using the RSTP protocol. As tests have confirmed, this however is limited by protocol immanent settings which either have to be accepted by application network design or worked around by proprietary solutions.

In Emergency mode, the network center nodes take over central network functionality in order to keep the network and safety essential services like VoIP and emergency guidance running independently from the central systems. Laboratory tests have shown that emergency switching and service assignment is working well. In the future, the large scale testing of the functions in an operating mine is pending as this is subject to availability of a large scale underground network which currently is being set up in different locations throughout Europe.

In an overall view, the system has the capability to significantly improve underground safety by cost efficient measures at the same time taking into account the most updated demands on functional safety.

References

[1] D. Brenkley et al., Mid term report RFCS project RFCS-CT2008-0001 "EMTECH", 2010, unpublished

[2] C. Müller, I. Szekely, (2010), Ethernet Communication for Detection of Emergency Locations and Dynamic Evacuation in Underground Infrastructures, Proceedings of the 12th OPTIM conference, Brasov, 2010

[3] U. Müller et al., Automatisierung von Bergwerksprozessen bei der RAG Aktiengesellschaft, Proceedings of the AIMS conference, Aachen, 2009, p177ff

[4] MineTronics GmbH, MIC Hardware User Manual, Ladbergen, 2010

[5] MineTronics GmbH, Network Application Setup Guidelines, Presentation Applications.odp, Ladbergen 2011, unpublished

[6] "Rapid Reconfiguration of Spanning Tree", IEEE 802.1w standard, 2006

[7] IEEE 802.1D-2004 standard, page 177, 2004

[8] MineTronics GmbH, RSTP Test Report, Ladbergen, 2011, unpublished

[9] D. Brenkley et al., Final report and deliverables RFCS project RFCS-CT2008-0001 "EMTECH", 2012, unpublished

[10] C. Müller, „Network based Communication in Mining and Tunnelling", Proceedings of the 17. Kolloquium für Bohr- und Sprengtechnik, Clausthal, 2010

[11] C. Ortega, "Fixed and mobile telecommunication systems in underground mines", Proceedings of the 33rd int. APCOM conference, Santiago/Chile, 2007, p563ff

[12] Manpage „snmpwalk", [online] available on 2012-01-20 at: http://linux.die.net/man/1/snmpwalk

[13] RFC3261 „Session Initiation Protocol", SIP