GLOBAL MINING GUIDELINES GROUP

GMG

20180921_Underground Mine Communications Infrastructure III-GMG-UM-v01-r01

UNDERGROUND MINE COMMUNICATIONS INFRASTRUCTURE GUIDELINES
PART III: GENERAL GUIDELINES

SUBMITTED BY
Underground Communications Infrastructure
Sub-Committee of the Underground Mining Working Group

VERSION DATE
21 Sept 2018

APPROVED BY
Vote of the Underground Mining Working Group
25 Feb 2019
and
GMG Governing Council
11 Mar 2019

EDITED BY
Purple Rock Inc.
26 Nov 2018

PUBLISHED
13 Mar 2019

DATE DOCUMENT TO BE REVIEWED
13 Mar 2024

PREPARED BY THE UNDERGROUND MINING WORKING GROUP
UNDERGROUND COMMUNICATIONS INFRASTRUCTURE SUB-COMMITTEE

CIM
ICM

ORGANIZATIONS INVOLVED IN THE PREPARATION OF THESE GUIDELINES

ABB, Accenture, Agnico Eagle Mines LTD, Alexander Proudfoot Africa, Alternate Futures PTY Ltd, Ambra Solutions, Anglo American Ltd, Aveva Group PLC, Barrick Gold, BBA, Bestech, BHP, Caterpillar, CBS Australia, CEMI, Cisco, CommitWorks, CSIR, Dassault Systemes GEOVIA, Datamine, De Beers Group Services, Deloitte, DesSoft, Deswik, DetNet, Dexcent, Dwyka Mining Services, E.C. MacDonald Inc., Echo Engineering Ltd, Epiroc, Excel Project Management, Glencore, Global IO, Gription, Hatch, Hexagon Mining, iMining, Inisys Africa BIM Solutions, Innovative Wireless Technologies, Ivy Tech Trading, JG & Co Management Consulting, JV Associates, KNS Communications, Komatsu, KPMG, Laird, Leoka Engineering, Maclean Engineering (Africa), Maestro Digital Mine, MetsTech, Micromine, MineRP, Minetec, Motorola, MST, Newmont, Newtrax Technologies, NL Technologies, North American Palladium, Northern Lights Technology, ORBCOMM, PA Spatial, PACE, Purple Group, Rio Tinto, Rockwell Automation, RPMGlobal, Sandvik Mining, Schneider Electric, SDMT, Sibanye-Stillwater, SITECH WA, Stantec, Technical University of Madrid, Telstra, Terrative Digital Solutions, Tetherco, University of Queensland, Thiess PTY Ltd, Thyssenkrupp, Torex, Transrupt, Tunnel Radio, University of Johannesburg, University of Pretoria, Vale, West Arm Consulting Group, Wipro, Worley Parsons, Yamana Gold

DISCLAIMER

Although these guidelines and other documents or information sources referenced at http://www.gmggroup.org are believed to be reliable, we do not guarantee the accuracy or completeness of any of these other documents or information sources. Use of these guidelines or the above documents or information sources is not intended to replace, contravene, or otherwise alter the requirements of any national, state, or local governmental statutes, laws, regulations, ordinances, or other requirements regarding the matters included herein. Compliance with these guidelines is entirely voluntary.

COPYRIGHT NOTICE

TABLE OF CONTENTS

1. FOREWORD

The Global Mining Guidelines Group (GMG) is a network of representatives from mining companies, original equipment manufacturers (OEMs), original technology manufacturers (OTMs), research organizations, and consultants around the world, creating multi-stakeholder working groups to systematically remove the impediments to building the safe, sustainable, and innovative mines of the future. To achieve this goal, GMG working groups establish focused projects to develop guidelines, such as this one, for the international mining industry. Draft documents are checked and approved by working group members, prior to approval by the GMG Governing Council.

Please note: if some of the elements of this document are subject to patent rights, GMG and and the Canadian Institute of Mining, Metallurgy and Petroleum (CIM, of which GMG is a legal entity) are not responsible for identifying such patent rights.

2. DEFINITIONS OF SYMBOLS AND ABBREVIATIONS

4G	Fourth Generation
ATA	Analogue Telephone Adapter
BBU	Broadcast Base Unit
BLE	Bluetooth® Low Energy
CCTV	Closed Circuit Television
DC	Direct Current
DMZ	Demilitarized Zone
DSS	Decision Support System
EIRP	Equivalent Isotropically Radiated Power
FDD	Frequency Division Duplex
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization
LAN	Local Area Network
LTE®	Long-term Evolution
MAC	Media Access Control
OEM	Original Equipment Manufacturer
OSI	Open Systems Interconnection (model)
OT	Operational Technology
PBX	Private Branch Exchange
PLC	Programmable Logic Controller
PoE®	Power over Ethernet
QoS	Quality of Service
RF	Radio Frequency
RFID	Radio Frequency Identification
RRU	Remote Radio Unit
RSTP	Rapid Spanning Tree Protocol
RTLS	Real-time Location System
TCP	Transmission Control Protocol
TDD	Time Division Duplex
UDP	User Datagram Protocol
UHF	Ultra High Frequency
UID	Unique Identifier
UPS	Uninterruptible Power Supply
UTP	Unshielded Twisted Pair
VHF	Very High Frequency
VOD	Ventilation on Demand
VOIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

3. KEYWORDS

Communications, Network, Security, Topology, Tracking Systems, Underground, Workstation Design

4. INTRODUCTION AND BACKGROUND

The rapid development of industrial and communications technology in recent years increasingly benefits mining activities around the globe and has affected nearly every facet of the mining process. Companies are rapidly deploying these new tools and applications to gain the associated productivity and financial benefits. However, they face a key challenge in that they require the appropriate infrastructure to support data communications technology in the mining environment, particularly underground mines.

Many new technologies developed and sold by vendors require high-speed digital networks to manage the increasing volumes of data generated in the underground mining environment. The data range from video and voice communications to vehicle telemetry, dispatch, and other critical systems and services. In the past, each vendor required separate networks for their proprietary solutions. Today, industrial control and mining solution vendors are moving towards a single standardized, consolidated communications infrastructure based on the digital Ethernet (transmission control protocol/internet protocol or TCP/IP) network framework—or at least are developing communications interfaces to allow their devices to interconnect with this type of network—in mine sites to improve production and cost optimization. This allows mining companies to run multiple services over a single backbone, thereby improving management while lowering deployment and support costs. The rapid shift from traditional, legacy analog systems (e.g., leaky feeder) to high-speed digital networks has created a lag in the knowledge and experience that is required to properly plan, design, deploy, and maintain such systems.

This guideline series is intended to provide a high-level view of the processes needed by mine personnel to meet planning and design requirements when creating or replacing

underground mine communications infrastructure. The series is intended to step the user through the general tasks and components needed to define the technical requirements for an underground communications infrastructure that supports mine services now and into the foreseeable future.

4.1 Parts Descriptions

The parts of this guideline series are arranged so the user learns a fundamental concept and then builds on their knowledge in each consecutive part. The following is a brief description of each part of the document series.

4.1.1 Positioning and Needs Analysis

Part I provides a general overview of the guideline objectives, audience, and mine communications maturity lifecycle diagram. This diagram provides a high-level overview of the services and supporting technology that is generally used in each phase of the mine lifecycle. The diagram initially shows business services and communications technology on the surface in the exploration phases and then shifts to the underground environment as the site develops.

4.1.2 Scenarios and Applications

Part II provides scenarios of practical applications in underground mining today and in the near future. The scenarios relate how different communications infrastructure designs can be used and combined to achieve key technology goals. The business services design requirements comprise a series of checklists to step through the general tasks and components needed Positioning and needs analysis for each phase of underground mine planning and development. The checklist helps mine personnel and contractors identify the appropriate network communications technologies to support required services and solutions.

4.1.3 General Guidelines

Part III (this document) is the core content of the guideline series. It provides the reader with an overview of the planning and design recommendations for underground communications development, some of the best practices used within mining environments, and where to find more information regarding digital communications, standards, and frameworks. This part also includes some guidance on technical best practices, security management, and remote operations.

5. SCOPE

This document provides an initial overview of the factors to consider when installing a network at an underground mine. It includes:

- General best practices as to how to decide on a specific network design and when to use given communications technologies
- Selection principles of network topology with respect to mining methods and mine design
- Communications coverage and tracking technologies in underground mines
- Managing network security
- Control room and remote workstation design

This document provides top-level information on these topics and also points a number of resources for further reading.

While not comprehensive, this document should provide a starting point for underground network selection and design. No two mines are identical; therefore, each situation will require a unique solution to provide the best communications infrastructure and technologies for that mine.

6. ADMINISTRATION: GENERAL GUIDANCE AND RECOMMENDATIONS

This section outlines important factors to consider during underground network selection and design, including local legislation, current network infrastructure, stakeholder engagement during planning, prioritizing needs, researching the options, and system selection. An overview of potential administrative tasks is provided, followed by examples of the communication regulatory bodies and legislative acts that are in effect in key mining jurisdictions around the world. Finally, common choices that must be made during communications infrastructure development are identified in a risk matrix along with pros, cons, and mitigative measures.

6.1 Potential Administrative Tasks

During the initial review stages of an upcoming project, suggested administrative tasks should include but are not necessarily limited to those discussed in Table 1.

6.2 Examples of Legislative Zones and Associated Codes

Appendix A provides examples of countries with mining activities and relevant regulatory bodies. The jurisdictions were selected to provide regional examples (i.e., Australia, Asia, Africa, and North and South America).

6.3 Risk Matrix

Choices that must be made during the development of a new communications network design come with associated risks. A risk matrix displays the pros and cons of each risk item, as well as proposed mitigation strategies (Table 2).

Table 1. Administrative Tasks During Initial Stages of Project Review

Task	Review questions	Regulations and factors to consider
Review legislation and safety standards.	How is the mine compliant or not compliant with the legislation? - Federal law - State law - National standard groups - National guidelines - Mine group policies/guidelines - Best practice guidelines/ documentation	- Privacy Act and considerations - Health and safety regulations - Air quality/emission sensing - Cybersecurity
	Is the mine compliant with the Corporate mandate?	
	What action(s) must be taken to ensure compliance?	- Fire suppressions for network/communications - Radio frequency licensing as required on surface and underground
Review the applications currently available and in operation on site.	Is there an existing operational communication infrastructure in place?	- Evaluate the benefit of reusing, upgrading,replacing, or moving the existing equipment to another location
	What software applications are currently being used on site?	
	What is the desired final outcome?	- Inventory/warehouse management - Atmospheric monitoring - Camp/whole site requirement (i.e., competing for global resources) - Cybersecurity applications - Diesel emissions - Disaster recovery applications - Emergency response - Geotechnical evaluations - Hazard reporting - Historian/data validation (local to devices and servers) - Network-enabled blasting systems - Personnel tracking and location – Radio frequency identification (RFID) - Proximity alert systems - Proximity detection/warning - Pumping - Risk assessments - Traffic control/traffic lights - Video monitoring, local and portable - Voice communication - Ventilation management - Ventilation on demand
Identify the current communication hardware.	What hardware devices are currently connected to the communication infrastructure?	- Video cameras - RFID reader(s) - Environmental and atmospheric monitoring devices - Instruments - Industrial controllers/Programmable logic controllers (PLCs) - Ventilation - Mobile devices
Determine if the communication infrastructure is currently sufficient to handle the current applications and associated hardware requirements.	Will the current applications continue to be used in the future? Can the communication infrastructure be expanded on and can it be upgraded to mesh with new technologies?	- Wi-Fi® - Mesh networks - Leaky feeder - LTE - Fibre optic

Table 1. (Continued)

Task	Review questions	Regulations and factors to consider
Set up meetings to engage with all stakeholders to define their individual "wish lists".	All stakeholders must be included in these discussions to determine what are their roles, what benefits them, and what are their "wish lists"	
	- Mine owner/superintendent	- Mine compliance - Increased production
	- Corporate	- Continuity being upheld between all mines owned - Central purchasing
	- Health and safety	- Health and safety standards and legislation being met - Increase mine safety - Reduce mine hazards - Decrease rescue response times in the case of an event
	- Mine rescue	- Personnel deployment efficiency - System deployment downtime
	- Operations - What are the benefits to mine operations?	- Equipment monitoring
	- Information technology/ operational technology (IT/OT) team (network management and security) and instrumentation	- Expansion of system with future mine growth - Equipment utilization efficiency - System criteria defined to ensure system security
	- Electrical team	- System automation requirements defined and met
	- Mechanical team	- Ease of deployment and maintenance - Required maintenance training
	- Union stewards	- Benefits to the union must be defined
	- Project management	- Ensure all stakeholders are informed and involved - Structure of the project - Timeframe of project - Internal deployment - Ensure the wish list ties in with project planning criteria and objectives
	- Finance	- Funding in the current budget - Capital expenditures or operating expenses
	- Mine	- Infrastructure requirements to expand or deploy systems
	- Engineering/geology/ geotechnical/metallurgy	
	- Survey teams	
	- Blast crew	
	- Materials and asset management	- Asset tracking
	- Ventilation Officer	- Automation
Prioritize the "wish list" to the approved projects.	What is the current communication mandate for the site? What will the future mandate/requirement(s) be?	- Financing - Budgeting - Operations
Build design, taking the criteria into consideration.	What is the end goal or objective?	Develop design criteria based on stakeholder input parameters and requirements (e.g.: bandwidth, latency, reliability)
Research existing solutions and original equipment manufacturers (OEMs).	What are the required specifications? What system fits the mine's needs? Is the system suitable and robust for underground conditions? Is the system easy to deploy? What is the length of operational disruption, if any?	

Table 1. (Continued)

Task	Review questions	Regulations and factors to consider
	What maintenance does the system require and by whom?	Electrical/mechanical/IT/OT staff OEM required Value Budget Warranty New regulatory changes tend to open new inexperienced OEMs in the mine sector
Create matrix/information for discussion and evaluation by stakeholders.		Decision and buy-in from all stakeholders
Follow the direction of decision outcome – Procurement stage.		OEM communication – tender/quotation/no bid Price negotiation Delivery/installation/start-up timeframes External and internal logistics
Hand off to procurement/ project management teams.	What should be included in the scope documentation?	Approved by all stakeholders

7. GENERAL BEST PRACTICES

The following section contains an overview of communications networks, including definitions of common terms, guidance for selecting industrial network technology, an overview of a commonly used model of communications technology layers, and several tables outlining the characteristics, applications, pros, and cons of different communications network technologies. The section closes with an overview of long-term evolution LTE®, a technology currently of great interest to the mining community.

7.1 Terms and Definitions

The following is a list of terms and definitions as they pertain to the data and communications field. They describe attributes that need to be considered when evaluating options and choosing a configuration that will be fit for purpose at the intended mine site.

- Adaptability: The ability to change with conditions, or the flexibility of a system to support new or evolving technology. Influencing factors include the inherent cost associated with changes versus the ability to support different applications with minimal modification.
- Attenuation: Loss of intensity in a data transmission, or signal depletion over the span or distance it travels, or through inherent design applications that limit the signal.
- Autonomy: In communications networks, a set of logic or "rules" programmed into the system to provide inherent routines for data processing, handle exceptions with misrouted data, and control traffic or data flow without manual interference by the end user.
- Availability: The amount of time in a defined period during which the asset is able to provide the needed function; a measurement of total usable time during which an asset is not being serviced or otherwise in an inoperable state.
- Capacity: The threshold limit of allowable data load at which a network can function without deleterious effects. Capacity can be defined as both a physical attribute that limits volume, or a performance attribute affecting quality. Care should be taken to clarify which type of capacity is addressed in context with the subject, e.g., quality of service (QoS; performance) versus restraints on peak demand (physical), which are similar but can vary slightly. A miscalculation in either can result in inadvertent cost and complexity overruns.
- Complexity: Pertaining to the size, makeup, equipment, media, and method in which a network functions with respect to each component of the system. The types of hardware and software can contribute to the overall complexity of the network, along with the types and numbers of nodes, access points, and redundant feeds. Installation, maintenance, and operation of the system can also be a contributing factor.
- Criticality: A ranking of importance of an asset determined by a series of factors regarding regulatory measures, safety, health, environmental effects, production impacts, ease of maintainability, reliability, and cost.

- **Durability:** The ability of an item to withstand environmental effects that might result in damage, loss of function, or diminished performance.
- **Interference:** Distortion, static, or signal interruption caused by other signals or ambient "noise" originating from outside sources.

Table 2. Example of a Risk Matrix

Risk item	Pros/benefits	Cons/challenges	Risk mitigation (general)
Use of non-current (older) equipment	- Cost savings - Legacy familiarity	- Non-compatibility issues with newer devices - Required upgrades increase costs - Maintenance contracts may not be available	- Balance cost of all new/current equipment against maintaining old equipment: based on lifespan and availability projections
Scalable solution	- Provides path for future growth	- Initial cost of solution may be higher - Ultimate mine size may be unknown	- Evaluate best estimate of final mine size; seek expandable network backbone that can be rolled out with mine development
Technology choice	- Offers solution for current applications/ needs	- Might not meet future applications/needs - Might not have sufficient longevity for the life of mine	- Select based on currently projected needs and equipment feature availability
Choosing a commercial grade product over an industrial equivalent	- Commercial products might be less expensive and easier to install	- Commercial product might not function as desired/designed - Retrofit costs - Commercial product might be unusable on an industrial scale	- Only apply commercial solutions in subcritical applications and expect to replace them more frequently
Requirements analysis	- Provides the necessary information/data to design proper solution	- May be difficult to align parties needs within budget	- Create spreadsheet outlining all applications and/or systems and their respective needs; seek overlap and compromise
Redundancy	- Robust network provides maximum uptime	- Additional costs - Failover complexity	- Prioritize critical applications for redundant capacity
IT/OT security	- Provides protection of network system via firewall(s)	- Costly - Complex configuration - May limit intersystem communication if not designed properly	- Work on social engineering and physical access security as on-going priority, cyber security to be developed continuously
System interoperability (expanding brownfield project)	- Expansions provide opportunities to replace old technology with new infrastructure	- New solution may not interoperate with existing solution	- Practice sequencing old and new modes of communication; plan to phase out old methods as production face moves
Proprietary systems	- Complete packages may be attractive with respect to cost and simplicity	- May hinder maintenance, access, and interoperability - Ensure full functionality is understood - The software company's longevity is not guaranteed so there is a risk of the need to switch to a different system entirely	- Ensure proprietary packages have standardized interface points and capacity - Ensure data from the proprietary system can be extracted in the event an application switch is needed in the future
Software/ hardware/ device compatibility	- Reduced IT/OT expense - Optimized network communications - Ease of new or replacement component integration - Simplified, robust cybersecurity model (reduced potential entry points)	- Effort is required to establish and enforce interoperability and compatibility standards across all business areas	- Include stakeholders and champions from all business areas, as well as vendors, in plans

- **Investment:** An expense, generally pertaining to the installation of a new system or asset with an economic evaluation, providing an economic return of funds by gained efficiency or improved use factors over time.
- **Labour:** Service provided at agreed upon terms supplied by in-house technician personnel or by vendor contract as determined by the individual site service model.
- **Labour Force:** All individuals of a population that are able to work at a given time.
- **Latency:** Delay in the transfer of data, also known as signal lag. This can be the result of factors such as digital processing time, transit time, data capacity threshold, or sensitivity to the type of media being transferred, for instance, video versus audio.
- **Lifecycle:** The period of effective economic use of an asset or system. Lifecycle analysis includes a consideration of procurement, start-up and commissioning plans, training plans, operating and maintenance strategies, staffing requirements, reliability, engineering processes, purchasing and stores processes with inventory requirements, and a decommissioning plan.
- **Maintenance:** The act of pre-emptively treating or reactively administering a repair to sustain an asset in a desired functional state. Maintenance can be performed during down periods, when the equipment is unavailable for use, or live, while the equipment is available for use.
- **Mobility:** The ability to access the communications network while moving throughout the mine.
- **Redundancy:** Tuplication of components or functions to create a backup or fail-safe mode in which to operate after a disruption. The objective is high availability.
- **Reliability:** A measure of the dependability of a system to perform at a defined quality. Reliability can be quantified using the frequency of failures over a given period (mean time between failures) and a corresponding measure of down time (mean time to repair).
- **Resiliency:** The ability of a machine or system to absorb the impact of the failure of one or more components or a significant disturbance in its environment while continuing to provide an acceptable level of service.
- **Safety:** 1) The use of security measures to offer insurance against harm, manipulation, or undesired access to a network and data; 2) a factor in the physical set up of the network that provides guarding, grounding, or other mitigation to reduce/remove hazards or prevent harm to people in contact with energized components.
- **Scalable:** The ability of a network or infrastructure to handle future network capacity growth. A scalable system is designed to manage and handle expansion or contraction as determined by the needs of the operation.
- **Security:** The use of encryption, access verification, or other safeguards to provide opposition to an outside breach of the system and protect the usability and integrity of the data. Security can include physical hardware and/or software technology.

7.2 Notes on Industrial Communication Technologies

The following factors should be considered during the development of industrial communication systems.

An underground communication network must exhibit redundancy under rugged working conditions. In addition to the rigorous requirements of hardware design and quality, a two-way communication architecture should be developed to provide high reliability. A reliable and robust communication system—usually composed of two parts: transceivers and a communication network—is necessary for transmitting audio and data information and tracking assets. For stationary units or worksites, cable-based (wired) communication systems are normally adequate; wireless systems should be used for mobile units.

There is a tendency for underground mines to use a single communication network for both voice and data. Older, single-function technologies required separate networks for each mode of communication; this is no longer necessary in modern mines. Standardizing communications and running multiple services along a single fibre backbone simplifies deployment and operations and can help reduce costs. When there is a fault in the network, redundancy such as ring-type architecture allows continued communication by looping the signals at the location of the fault.

Even if the communication system focuses on the targets set during short-term planning, it should include instruments that could satisfy requirements for optimal or near-optimal solutions for the long term.

7.3 Network Selection and Design

The type of network that will be suitable for a specific underground mine is dependent on several factors, including:

- The stage of operation of the mine (e.g., development, commercial production, or near end of life)
- The purpose of the network: Emergency response, tracking, ventilation on demand (VOD), environmental monitoring, and collision avoidance, or a combination of applications
- The mine's budget for the network

The type of application(s) required will dictate which communication infrastructure is necessary: wired, optical,

radio, or a hybrid system. The more complex an application is (e.g., collision avoidance), the more complex the design and implementation will be. Additionally, any applications that might be desired in the future must be considered in advance so that, if funds allow, the selected communications infrastructure can support the expansion.

Once the applications and communication infrastructure have been selected, the characteristics of the various technologies must be considered to design the network.

7.4 Seven-Layer Model for Networking

To ensure that network equipment can communicate over different types of media, such as fibre optic and copper local area network (LAN) cables, and to future-proof the network to allow for new data transfer and management protocols, a layer approach is recommended. The International Organization for Standardization (ISO) developed the open systems interconnection (OSI) communications model. It divides network communication into seven layers (Figure 1). Layers 1–4, the lower layers, are mostly concerned with moving data around. Layers 5–7, the upper layers, contain application-level data. The communication infrastructure in an underground mining environment will use mainly layers 1–4.

The overall performance of a communication system is dependent on the characteristics/performance of each individual layer; one layer may limit the performance of the overall system, or of a specific application for which the system is built. It requires skill and experience to properly define and select each layer of the communications network for peak performance.

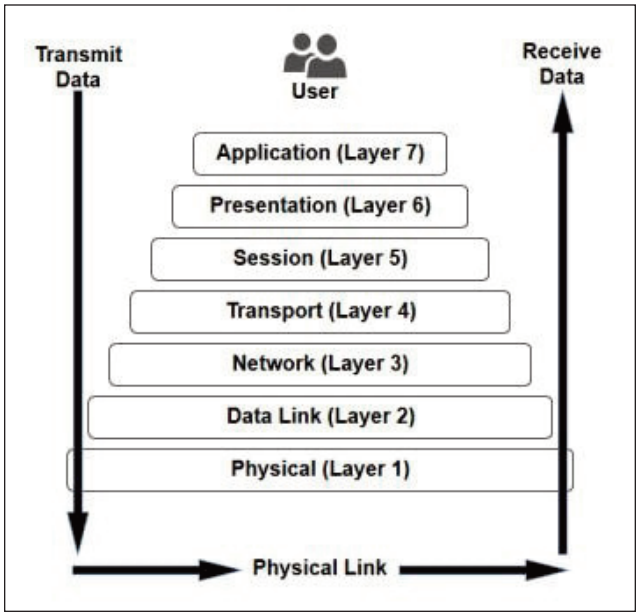


Figure 1. Seven Layers of the Open Systems Interconnection (OSI) Model

Networks operate on one basic principle: "pass it on". Each layer takes care of a very specific job, and then passes the data onto the next layer. Layers have autonomy, so each layer is fully independent and able to complete the functions assigned to that layer. The OSI model takes the task of internetworking and divides it up into a "vertical stack" of seven layers. Control is passed from one layer to the next, starting at the application layer (layer 7) at one station, and proceeding to the physical layer (layer 1), across the network to layer 1 at the next station and back up the hierarchy to layer 7.

A few examples of layers 1–4 will help to describe their function within the context of a mine network:

Physical (Layer 1)

The physical layer consists of the electronic transmission technologies of a network. These include the cables and electronic circuits that make up wired networks. In over-the-air networks the physical layer is the radio transmitters, receivers, and allocated frequency bands in the electromagnetic spectrum.

Data Link (Layer 2)

The data link layer provides the functional and procedural means to transfer data between network entities and can provide the means to detect and possibly even correct errors that can occur in the physical layer. The data layer at one station communicates with the data layer at another station via the physical layer. The data link layer controls access to the physical layer to manage data and prevent collisions (data collisions occur when two devices try to talk at the same time on the same physical layer). Examples of the data link layer are Ethernet, token ring, and Wi-Fi®. Addressing in this layer is local only.

Network (Layer 3)

The network layer provides the means to transfer variable-length network packets from a source to a destination via one or more network paths and can transfer data across different networks and to destinations that are not necessarily local. Because it is involved with the routing or directing of data traffic, the network layer deals with addressing systems. The network layer responds to service requests from the transport layer (layer 4) and issues service requests to the data link layer (layer 2). An example of the network layer is IP.

Transport (Layer 4)

This layer provides services such as connection-oriented communication, reliability, flow control, and multiplexing. In layperson's terms, this layer is responsible for ensuring that data arrive at their destination. It is also accountable for scheduling the rate that data is added to the network layer (layer 3). Examples of the transport layer are TCP and user datagram protocol (UDP). The main difference

between TCP and UDP is that TCP guarantees delivery of data traffic, while UDP does not guarantee delivery; however, UDP tends to be faster and more efficient for order-critical data streams like video and audio.

The following is an analogy for layers 1–4:

Person A wants to send a series of letters to person B. Because these letters contain critical information, person A is going to use registered mail to track the letters and ensure they are delivered (TCP; layer 4). The letters have a destination address and a return address. The postal company use the destination address to determine which postal branch to send the letters to (network; layer 3). The postal company uses the public infrastructure to move the letters between the branches and from the branch to the end destination. They must comply with the rules of the transport system they use (e.g., the postal truck must follow the road rules of the area it is travelling in (e.g., stop at red traffic lights; data link; layer 2). The roads and the vehicles the postal company uses are the physical layer (layer 1).

Although the communications infrastructure of an underground mine uses mainly layers 1–4, layers 5–7 still play a part.

Session (Layer 5)

The session layer is mainly concerned with managing connections between local and remote computers: opening, managing, and terminating sessions cleanly.

Presentation (Layer 6)

The presentation (or syntax) layer allows applications-level entities to communicate, even if they are not otherwise compatible. In this way, the presentation layer can be seen as somewhat of a translator, providing mapping between the languages used by different programs.

Application (Layer 7)

The application layer supports applications and end users. This layer facilitates communication when an application or an end user needs to transmit data through the network.

7.5 High-Level Communications Infrastructure Decision Matrix

A number of communications infrastructures are available for use within mines. To decide which infrastructure (or combination of infrastructures) is best for a given mine, a matrix with high-level characteristics may be helpful (Table 3). This table outlines common technology solutions for communications networks, provides a broad description of what each technology does, indicates typical applications, and summarizes benefits and detractions for each potential solution.

7.6 Technology Specifics

Consult Appendix B for further specifics about common network technologies and communications systems.

Table 3. High-Level Communications Infrastructure Matrix

Solution	Description	Applications	Pros	Cons
Analogue telephony	Traditional private branch exchange (PBX) telephony system	- Voice communications - Voicemail - Capable of connecting long distances between phone sets	- Low-cost cabling - Easier maintenance - Trunk cable, typically located in the shaft, is a high-count cable	- Voice only - Initial configuration is complex
Voice over Internet protocol (VOIP)	Voice and multimedia communications over an IP network	- Voice communications - Video conferencing - Audio conferencing - Voicemail - Wireless communications	- Uses unshielded twisted pair (UTP) cabling to connect phone sets - Uses existing IT network equipment to connect phone sets - Can integrate with traditional copper cable solutions (digital or analogue) with the use of voice gateways or analogue telephone adapter (ATA) devices - Single system to manage	- Complex system - Requires power over Ethernet (PoE) network equipment to provide power to devices such as phone sets
Digital radio system	Two-way radio with digital technology	- Mobile voice communications - Voice communications - Tracking applications such as man down alerts - Most brownfield underground installations use radio frequency (RF) based two-way radio system over leaky feeder	- Capable of data communications - Can be used for man-down applications	- Data rates are lower than for IP solutions - RF licensing may be required in some locations - High latency

Table 3. (Continued)

Solution	Description	Applications	Pros	Cons
Wireless network (Wi-Fi)	Wireless local area networking with devices based on the IEEE 802.11 standards (Institute of Electrical and Electronics Engineers, 2018)	- Location-based services - Mobile communications (voice and data)	- Extension of IT network equipment - Provides mobility for users - Location-based services can be used	- Complex to configure - Requires site survey and planning prior to installation - Limited coverage in underground installations
Cellular network (LTE)	High-speed wireless communication for mobile devices and data terminals	- Voice, data, and video - Multimedia	- Better signal propagation compared to 2.4/5.0 GHz Wi-Fi in underground installations	- RF licensing required for use in surface and underground installations
Wide area network WAN)	Network covering a large geographic region	- Interconnectivity between data centres	- High bandwidth	- Generally involves leased circuits - Complex configurations
Local area network (LAN)	Localized interconnection of computers and network devices	- Interconnectivity of network equipment - Interconnectivity between peripherals	- High speed - Low cost - Ease of setup - High bandwidth	- Larger systems require complex configurations

7.7 LTE® as a Communications Infrastructure

LTE is an IP-based wireless communications technology that constitutes an OSI model Layer 4 (transport; Figure 1). LTE is a relatively new technology in the underground mine environment that offers new applications and potential performance and cost benefits for the industry. In this guideline, LTE refers to technologies such as fourth generation (4G) cellular networking technologies and beyond. LTE is most often compared to Wi-Fi (Table 4).

Table 4. Comparison of LTE and Wi-Fi technologies (adapted from Ambra Solutions inc. [2018])

Parameter	LTE	Wi-Fi
Bands	Licensed bands: - Allows carrier aggregation - Free of interference - Expensive or nonexistent band licensing	Unlicensed band: - Subject to interference - Free to use
Power	Maximum base station equivalent isotropically radiated power (EIRP): between 1 W and 4 W	Limited to 1,000 mW EIRP by Industry Canada/FCC, often only 100 mW in the rest of the world.
Signal strength	Lowest working signal strength: –115 dBm	Lowest reliable signal strength: –85 dBm
Latency	Latency remains constant as network traffic increases	Latency increases as network traffic increases
Duplex scheme	Frequency division duplex (FDD) and time division duplex (TDD) - Can use separate channels for uplink and downlink	TDD - Uses the same channel for uplink and downlink
Mobility	Full mobility up to 300 km/h	Limited mobility ("break before make")
Quality of Service (QoS)	Superior end to end QoS capabilities natively implemented in the standard	Limited QoS capabilities
Range and compatibility	- Different LTE standards around the world - Some are compatible with commercial cellular LTE networks	Limited range resulting in high number of access points to manage – Wi-Fi is a universal standard
Usage fees	Packet billing per use if connected via cell phone providers, or requires licensed frequency band from regulator for exclusive use	Free to use
Equipment costs	More expensive initial equipment costs (up to 10 times those of WiFi)	Inexpensive equipment costs

LTE can be used in underground mines for most pertinent applications, including broadcast communications, peer-to-peer communications, push-to-talk, asset and personnel tracking, and remote/autonomous control of equipment.

An LTE network consists of a primary access point installed at a fibre optic backbone connected to sequential (repeater) antennas installed across the span to be covered, with each antenna connected to the next via coaxial cable. Unlike Wi-Fi access points, the repeater antenna do not have to be configured, making them easy to install.

8. GENERAL TOPOLOGY

This section includes discussions of mine structures, idealized communications topology, the pros and cons of different topologies, and failure modes.

Mine topology has a direct effect on where and how a communications system can be designed, installed, and used, so the two topics are discussed together. Mine topology itself is influenced by the type of mining in questions, including:

- Mineralization in orebody and surrounding area
- Temperature
- Humidity
- Gasses present

These factors will influence the mine structure, the communications network, and the hardware accessories (e.g., enclosures, cables).

8.1 Types of Mining

Mining can generally be broken down into either surface (open cast, open pit) or underground. In either case, orebodies can be broadly categorized by rock type as one of the following:

- **Hard rock:** Mineral extraction is typically conducted by drill and blast, or by boring in the case of medium-hard rock. Examples of hard-rock minerals are native nickel, copper, and gold.
- **Soft rock:** Mining is typically conducted by means of mechanical excavation and without the use of explosives, using machines such as continuous miners, shearers, and roadheaders. Examples of soft-rock minerals are salt (used as road salt), potash, coal, and trona.

Soft-rock mines tend to be relatively flat, single-horizon orebodies or seam deposits, whereas hard-rock mines tend to be irregularly shaped orebodies that are mined across multiple horizons or levels.

8.2 Underground Mining Methods

Underground mining methods can be generally classified as one of three types, differentiated by the wall and roof supports used, configuration and size of production openings, and direction of mining:

- **Unsupported:** No artificial pillars; used in flat, tabular, bedded horizontal deposits or seams; e.g., room and pillar
- **Supported:** Used in weak rock structures or steeply dipping deposits; e.g., cut and fill stoping, sublevel stoping
- **Caving:** Used for dipping tabular or massive deposits; e.g., sublevel caving

Access to underground mines may be via:

- Ramp or decline leading from a portal on the surface to the underground workings
- Vertical shaft from the surface to one or more levels underground
- A combination of shaft(s) and underground ramps that connect two or more levels

Hard-rock mines are more commonly mined using drifts (tunnels) driven through the host rock to the adjacent orebody, where excavation is via drilling, blasting, and mucking of broken rock. Typical hard-rock mines consist of a series of shafts, ramps, drifts, and stopes across multiple levels designed to access the orebody (Figures 2–4).

Given the hazardous and potentially destructive nature of hard-rock mining (i.e., drilling and blasting), it is difficult to install and protect sensitive networking equipment and cables; however, network-enabled monitoring equipment such as extensometers and sloughmeters can collect crucial information as a mine progresses. One solution may be to consider a wireless mesh network (Mine Design Technologies, 2018), where instruments can be connected to wireless nodes throughout the mine without the need for extensive equipment or cabling.

The topology of hard-rock mines often consists of 5 m × 5 m tunnels (e.g., massive sulphide deposits) or smaller 4 m × 2 m drifts (e.g., tabular mining) that lead to mining stopes where the ore is extracted. Access to these stopes is commonly via main travelways to a single access drift leading to the face (or stope).

Many methods exist to mine an orebody; the selection of the best method is based on the physical characteristics of the orebody. In hard-rock mining, the Hartman chart can be used to select the appropriate mining method (Figure 5). Each mining method results in different tunnel patterns, hereby referred to as the "mine topology".

In North America, soft-rock mines are typically a single horizon orebody and are very expansive, with long, wide tunnels (and openings) supported by pillars. The resulting (typical) mine topology, called "room and pillar", may look similar to a checkerboard (Figures 6–7). In this mine topol-

Courtesy of Atlas Copco (Now Epiroc)

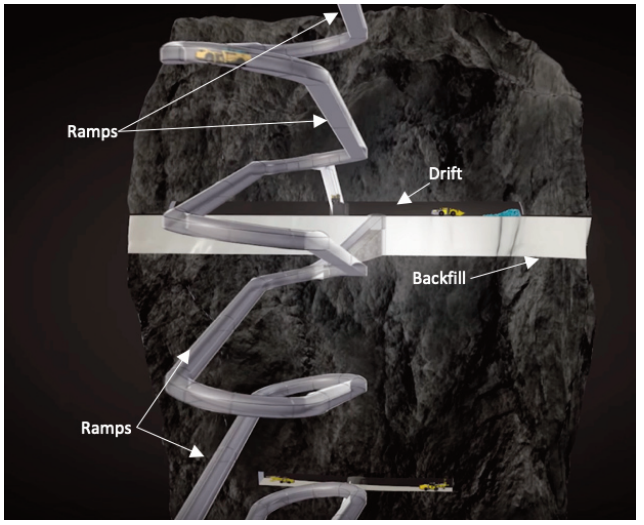


Figure 2. Sublevel Stoping in a Hard-rock Mine.

Courtesy of Atlas Copco (Now Epiroc)

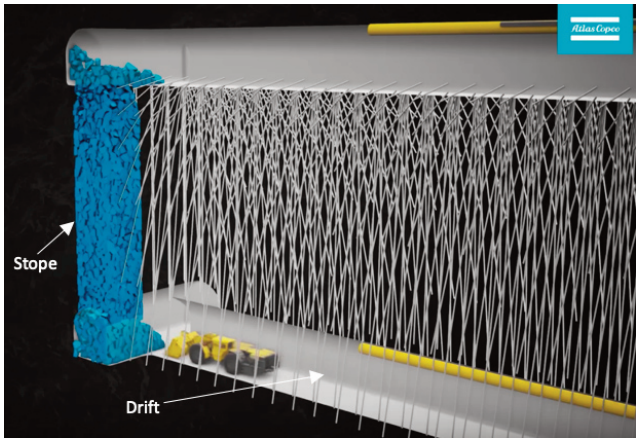


Figure 3. Detailed View of Sublevel Stoping in a Hard-Rock Mine.

Courtesy of Atlas Copco (Now Epiroc)

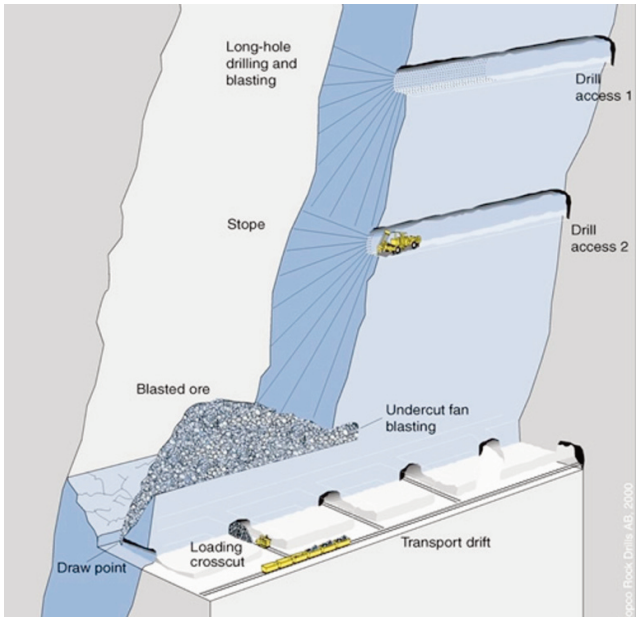


Figure 4. Example of Underground Hard-Rock Mining.

ogy, normal travelways are established from the shaft station (for an underground shaft mine) to the working face (heading, room, or stope). These are generally the main paths used to move people, material, and equipment in and out of the mine. Installing permanent infrastructure in these areas allows the mine to establish pervasive communications along these travel-ways with the ability to build redundant links across alternate paths around the pillars. These redundant paths can be designed using fibre optic cable, coaxial cable, copper wire, or wireless mesh nodes. Given that drilling and blasting is normally not used in soft-rock mining, damage to equipment at the face is reduced compared to hard-rock mining; however, it is important to recognize that damage resulting from scaling, mucking, and vehicles moving in and around the face is still possible. The placement and mounting of cabling and hardware should consider the potential for damage from activity in the area during active mining.

8.3 Ideal Network Topology Models for Underground Mines

Underground communication can be challenging to design. It is often a best practice to be flexible and leverage more than one topology within a mine to overcome constraints. Four main network topologies are commonly used in underground mines (Figure 8):

- **Bus topology:** All nodes are directly connected to a single linear cable
  - Example: Leaky feeder (radiating cable)
- **Ring topology:** All nodes are connected via a ring of cable
  - Example: resilient Ethernet
- **Mesh topology:** Network in which each node has a direct connection to all others; in a partial mesh topology, some nodes are connected to all others, while others are only connected to those nodes with which they exchange data; may be wired or wireless.
  - Example: the Internet
- **Star topology:** All nodes are connected to a central hub via a dedicated path
  - Example: traditional Ethernet

Table 5 describes some of the pros and cons of the network topologies described above.

8.3.1 Bus Topology

Bus topology is effective for a small network. In this design, each device is connected to a common cable. An advantage to this is that it requires less cable than the star topology and is easy to extend as a mine expanded; however, in a larger network, many devices can slow down data

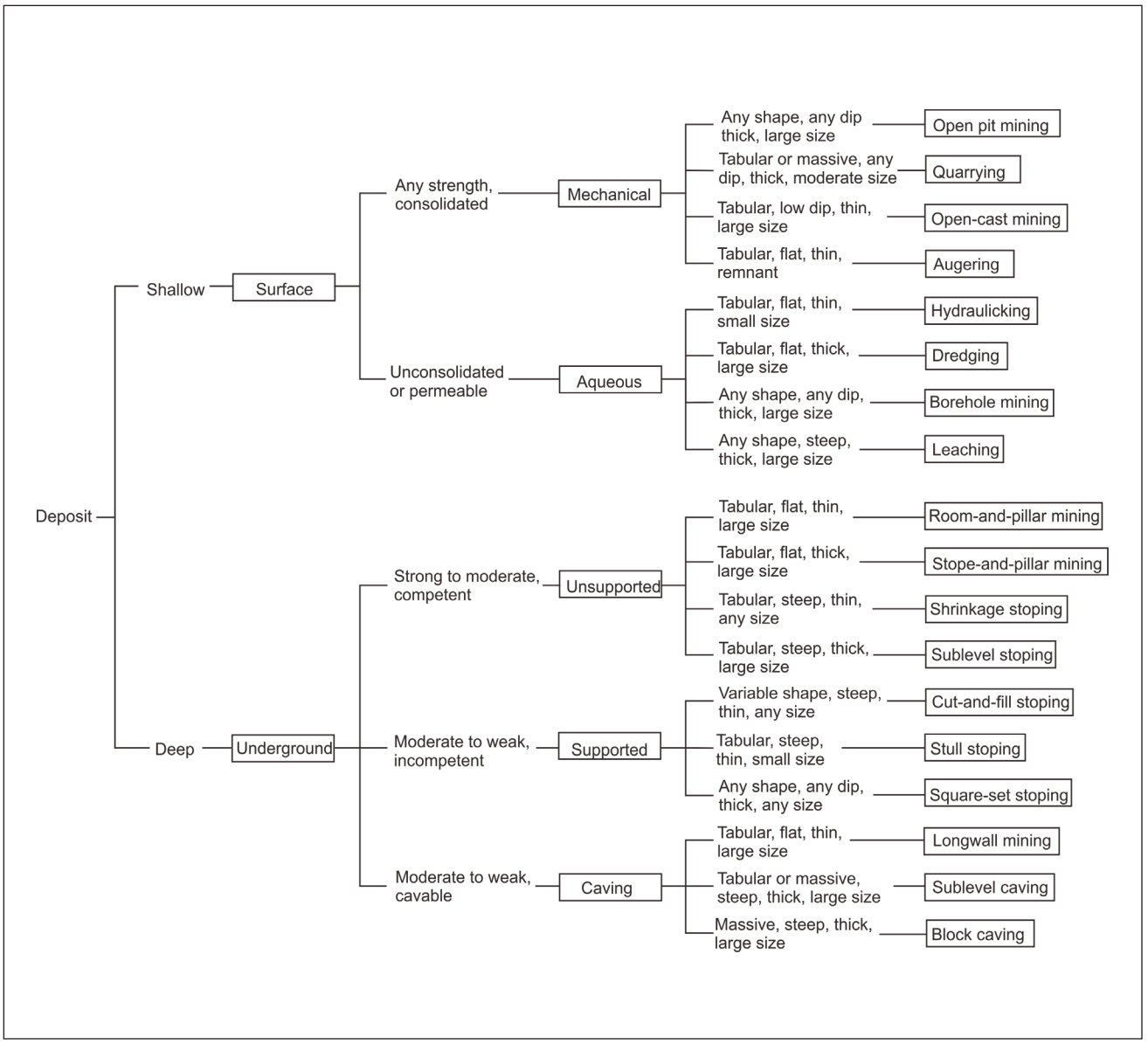
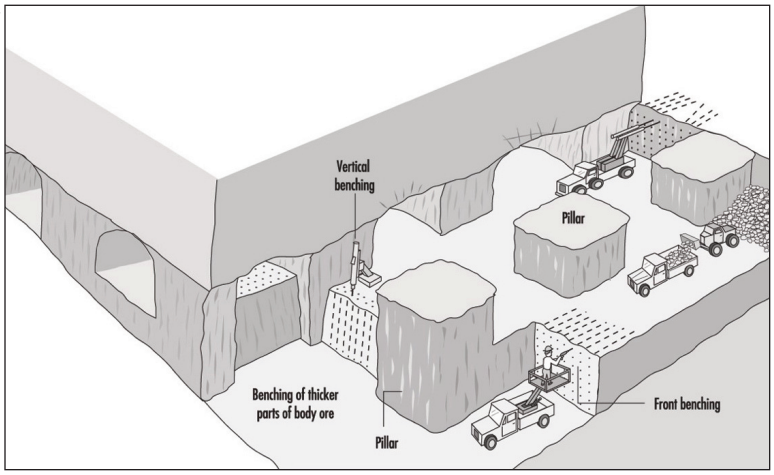


Figure 5. Hartman Chart for the Selection of Hard Rock Mining Method (adapted from Hartman, 1987)



From the International Labour Organization Encyclopaedia of Occupational Health and Safety.

Figure 6. Room and Pillar Topology Schematic for a Coal Mine.

Courtesy of Agrium

Figure 7. Potash Mine with Room and Pillar Topology.

Table 5. Pros and Cons of Applying Different Network Topologies in an Underground Mine

Topology	Pros	Cons
Bus	- Simple design - Simple to install - Effective for a small network - Can be expanded as the mine develops the tunnels - Usually the communication cable also carries the energy to feed the nodes - A small number of linear hops using Wi-Fi can be useful underground (e.g., delivering Wi-Fi to the mine face by bridging back to the more permanent wired network)	- Not resilient to failures - An outage or cable cut at one point can impact all downstream communication - Must be reorganized when technical limitations are met - High latency at the end of network because data packets are repeated from node to node - An increase in the number of devices can slow down a data transfer
Ring	- Data are injected or delivered from any node on the network - If one side of the ring breaks, data may be received from the other side - Resilient to outages or damage - Very high speed networks, using single-mode fibre optic cables	- Expensive equipment - Both sides of the ring may be in the same cable and in the same tunnel, thus have the same vulnerability to failure - Fibre optic networks require more time and expertise to repair
Mesh	- Wireless; no need for communication cable - Less chance of damage because there are no communication cables	- Generally not suited to linear tunnels - Still requires a power cable - Battery-powered systems require replacing/recharging batteries regularly - High latency at the end of the network because data packets are repeated from node to node - Because there is only one route between nodes, there is no real backup route - Because each node is dependent on the previous one, the risk of failure increases with distance from the data source - Needs constant maintenance and monitoring to be effective
Star	- Each leg is autonomous - Other legs remain operational if one leg fails - Each leg has its own performance characteristics - Preferred architecture for a mine with a shaft and multiple levels; one level is one leg - Can be implemented using Ethernet cat 5-6, coaxial, or fibre optic cables - High performance due to dedicated path to each node	- Each leg is a daisy chain system - The mine must be designed to allow for a centrally located hub. - Difficult to implement in a mine with a ramp, especially while under development - Long tunnels require more cable - Direct current (DC) and RF losses in cables limit distances to the last node

transfer. Additionally, if the main cable breaks, the entire system is disabled.

8.3.2 Ring Topology

Ring topology is one of the more frequently used topologies in underground mining. It has the benefit of simplicity and very fast recovery times. Ring topology is commonly deployed as a more complex structure in which multiple rings interweave. Figure 9 shows a typical ring; when all connections between the switches are functional, one of the links will be disabled so that the data only passes through the ring once. If any of the cables are cut, an alternate pass is made available.

A typical use of this topology is in a decline or shaft combined a with second ring from an on-level switch into the workings. In this example, the forward and return path of the cable are in the same physical space; however, they are could be run on the left and right side of the roadway, adding some protection from damage (Figure 10). Where possible, the physical cable path should be separated. Figure 11 shows an example where the return path is run through a borehole to a lower level. This will grant greater

protection from catastrophic events such as roof falls.

8.3.3 Mesh Topology

Wired mesh topologies are rarely deployed in underground networks because they are only effective if multiple redundant network paths exist. This is difficult to achieve within the layout of most mines. A further drawback is that a mesh topology needs constant maintenance and monitoring to be effective.

Wireless mesh solutions are easier to deploy; however, they cannot effectively replace a cable-based backbone network. In situations where it is difficult to maintain a fixed infrastructure due to blasting or other hostile activity, a battery-powered wireless mesh network can be a good fit. These devices can connect wirelessly to a fixed wireless access point and then "dropped in" as needed to extend the network, making for a flexible solution and offering a mobile extension to the network. There is a limit to the number of mesh nodes that can be deployed because of latency over longer distances.

Figure 12 shows a wireless mesh network formed with mobile Wi-Fi nodes (red). The nodes are battery operated and can be removed prior to blasting. Overall infrastructure is greatly reduced due to its flexibility, allowing the network to be deployed in specific locations on an as needed basis. The network is very resilient because it can bypass failed nodes and remain viable at reduced bandwidths.

8.3.4 Star Topology

This topology is common in underground mines. In most cases a protocol called rapid spanning tree protocol (RSTP) is deployed as a mechanism for redundancy. The recovery time is relatively slow—anywhere from three seconds to several

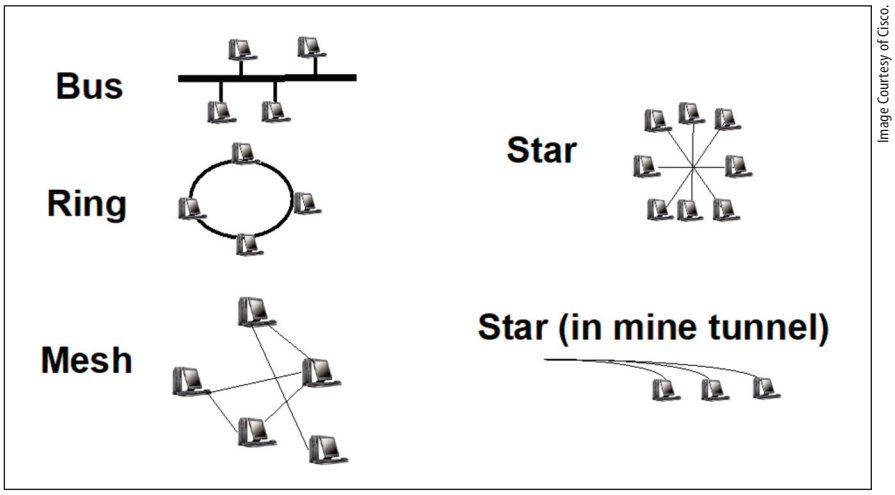


Image Courtesy of Cisco.

Figure 8. Four Key Network Topology Types. The Image of the Computer Represents a Station or Point of Connectivity on the Network. The Star (In Mine Tunnel) Represents the Difference Between the Network Logical Operation and Physical Layout.

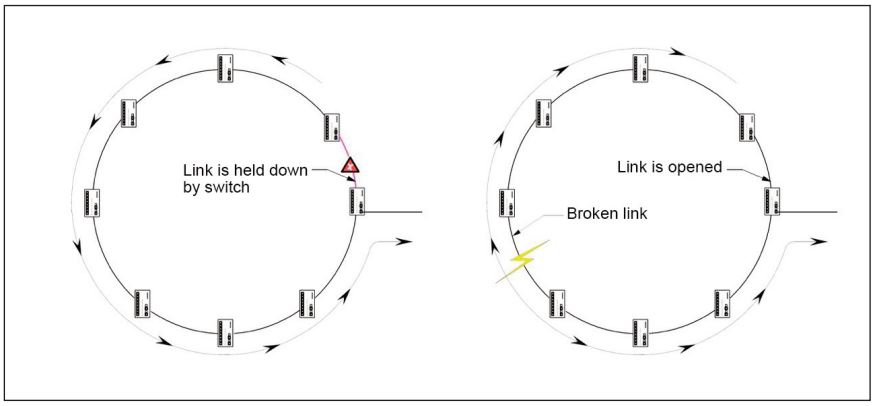


Figure 9. Typical Ring Topology. When Fully Functional, One Link of the Ring is Disabled; if Another Link Becomes Damaged, the Disabled Link Becomes Functional to Allow Data to Pass to and from all Nodes in the Ring.

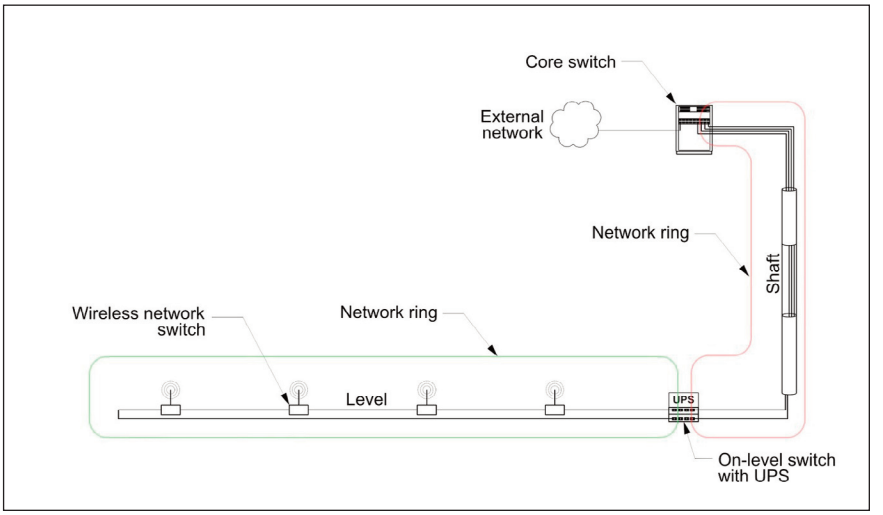


Figure 10. Ring Topology Networks (Red and Green) in a Mine with Forward and Return Paths in the Same Physical Space

minutes—depending on the size of the network and type of component failure. This topology is not recommended for networks that need fast recovery such as critical automation systems; however, it is well suited for many applications such as underground office areas. In a star topology, multiple redundant connections between network switches can exist if RSTP is implemented. The RSTP protocol will disable all duplicated links until the active link is broken. This process is fully managed by the switches and has little overhead; however, the process of recalculating the new path takes some time and is not suited for mission critical applications.

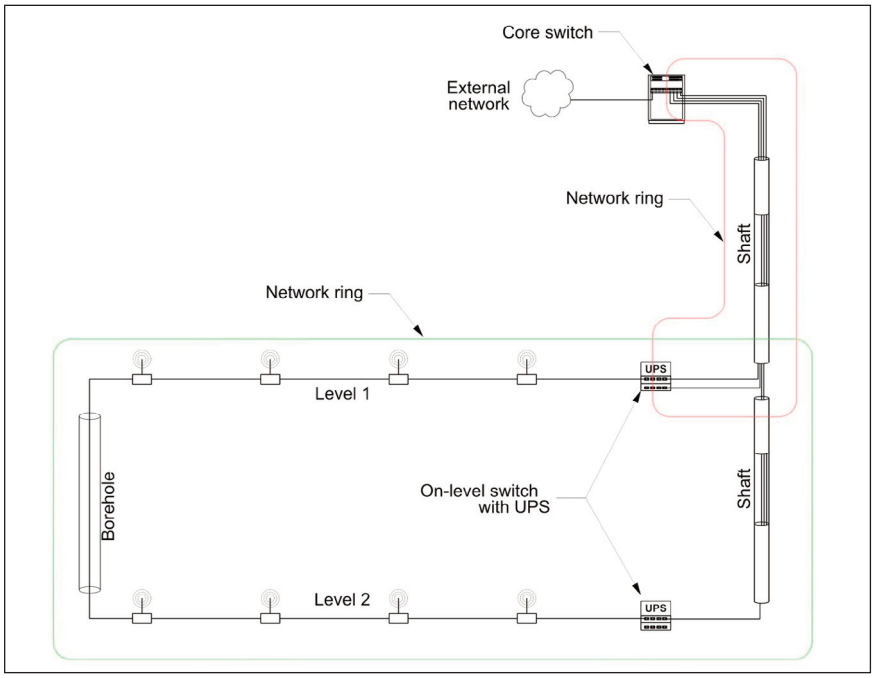


Figure 11. Ring Topology Networks (Red and Green) in a Mine with Forward and Return Paths in Separate Physical Spaces

In Figure 13, a star topology is deployed on level 1, which is an office area. Two on-level network switches connect multiple end devices. The switch near the shaft is connected via a ring topology to the server room at the surface. This switch extends the network to a secondary on-level switch. This connection is duplicated by a parallel link; however, the RSTP disables one of the links. In the event that the active link fails, the second link would become active. This takes several seconds because the switch needs to calculate the new path. In contrast, the ring connecting the first on-level switch to the surface would take less than 30 ms to recover in the event of failure. A ring network connects nodes on level 2.

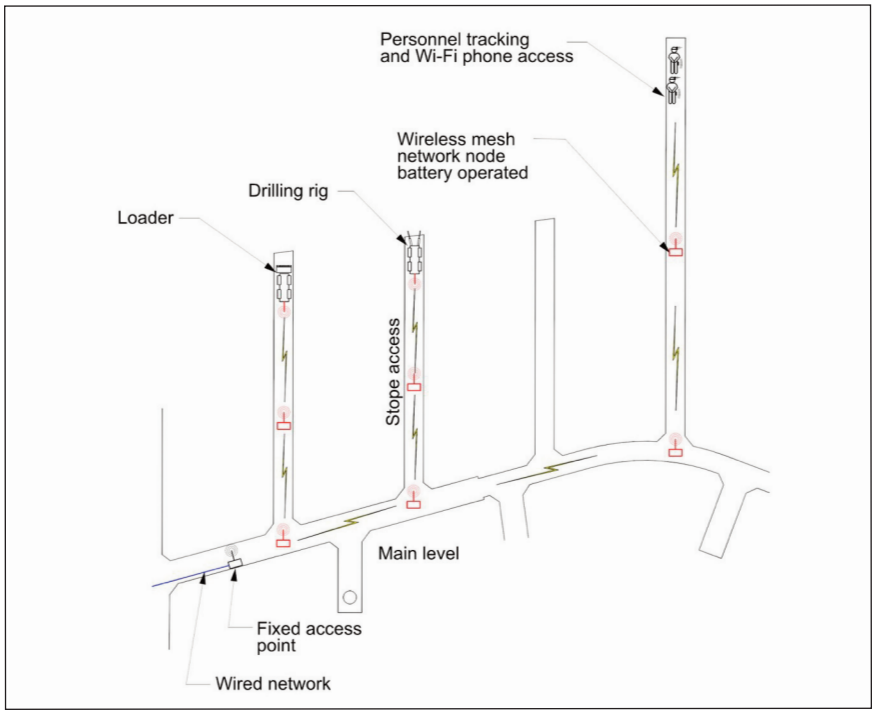


Figure 12. Mobile Wireless Mesh Network (Red Nodes) Connected to a Fixed Access Point (Black)

8.4 Integrating Mine and Wireless Communications Topologies

The mine topology impacts the design, installation, and use of any communication system. Additionally, different component suppliers may have limitations to their equipment depending on the selected/primary network topologies.

In the mine shown in Figure 14, fibre optic cable can be installed in the main shaft and broken out on each of the main levels. As mining progresses onto each level, permanent infrastructure can be extended along travelways using a star topology from the level electrical substation, where a network switch may be connected via the main fibre optic cable.

Ideally, a redundant run of fibre optic cable should be run via a separate ventilation shaft from each level to the surface (Figure 15). Likewise, if the sublevel topology permits, a redundant run of fibre optic or coaxial cable can be run to eliminate a single point of failure in the event of a cable cut.

For example, wireless infrastructure can be installed along the main travelways, interconnected by fibre optic, copper wire, or hybrid cables. Once developed, this infrastructure remains as a permanent means of accessing the developing drifts in the mine, where new infrastructure must be installed to follow the advancement of mining. It is impractical to install permanent, wired infrastructure in stopes where active drilling and blasting is taking place until mining advances beyond the range of impact from blast percussion and damage from flying rock. Extending wireless coverage in active drilling areas can be done temporarily by

- Rolling out temporary cabling to power and connect temporary access points to fixed infrastructure
- Using self-powered (or powered if power is available) portable access points
- Using a series of self-powered (or powered if power is available) mesh nodes to extend coverage to the stope during activities such as drilling, mucking, and ground support work (Figure 16)

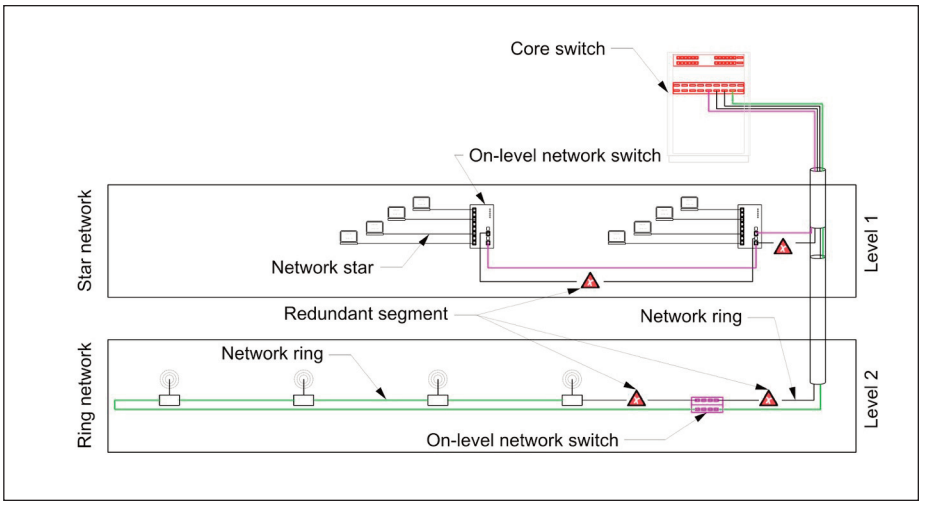


Figure 13. Star Topology Implemented on Level 1 in a Two-Level Underground Mine. Level 2 Shows a Typical Ring Topology. Ring Topology is also Used to Connect Both Levels to the Surface Server Room.

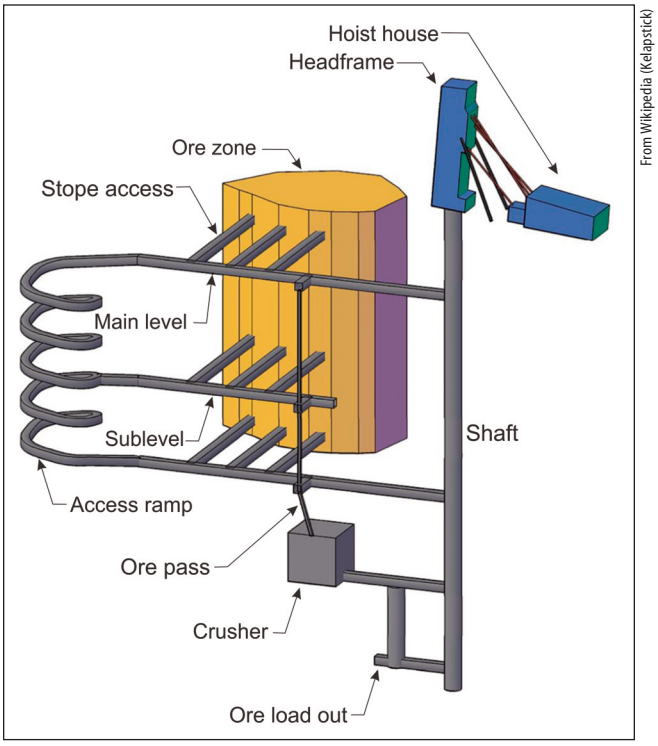


Figure 14. Schematic of Underground Hard-Rock Mine.

8.4.1 Intrinsically Safe Devices—Special Considerations for Coal Mines

Because underground coal mines generally have methane gas and coal dust present, all electrical and electronic devices must be designed for intrinsic safety to minimize the risk of sparks, which could ignite methane gas or coal dust in the mine. Regardless of what communications technology is selected, regional legislation must be adhered to and only sanctioned "intrinsically safe" devices must be used. Intrinsically safe devices might also be required in non-coal mines that contain fire hazards. It is important to verify if the mine in question is classified as such prior to selecting a communications solution.

8.5 Choosing IP Network Infrastructure

The physical architecture of IP network infrastructure in underground mining operations varies greatly from that used in other industries. In most cases, the design of the mine's tunnels limits the physical layout of the network. For example, roadways are designed so that there is only one way in and one way out, making it difficult to provide a redundant network path for the data cable. In addition, blasting at the face poses physical risks to the network, making it difficult to maintain infrastructure near the face. Arguably, the cable could be returned in the same roadway; however, this would provide little protection in the case of a major roof fall. In

Courtesy of Terrative Digital Solutions

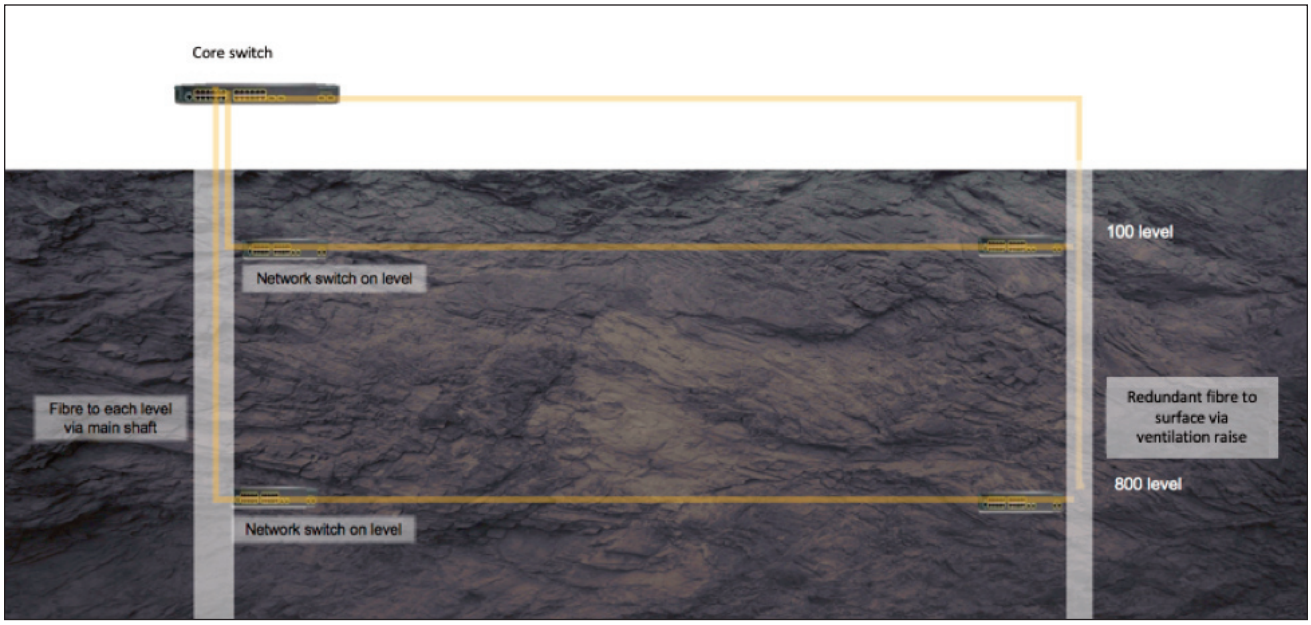


Figure 15. Redundant Fibre Topology.

some cases boreholes are present between levels or roadways and can provide a return path; however, it could be difficult to repair the cable in case of a failure within the borehole and geological instability can make the use of boreholes difficult or costly.

Courtesy of Terrative Digital Solutions

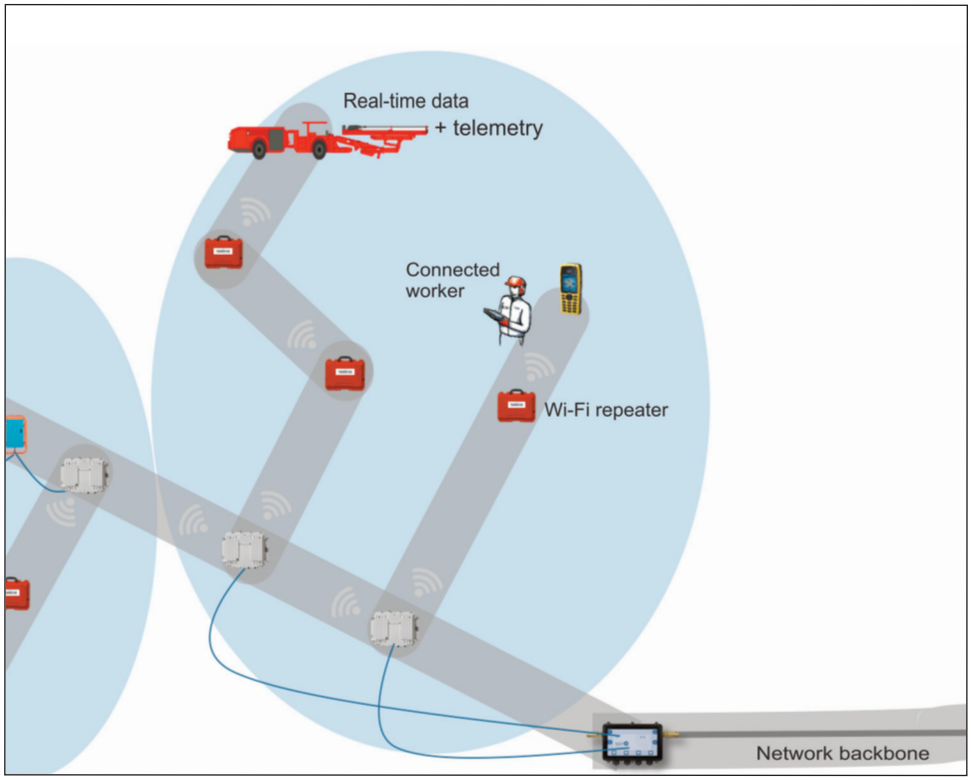


Figure 16. Extending Wi-Fi to the Mining Face. White Boxes Represent Permanent Communications Infrastructure, which can Communicate with Temporary Wi-Fi Repeaters (Red) until Permanent Devices can be Installed.

Each mine must take an individual approach to ensure a reliably built network; however, there are some common architectures that can be used alone or in combination in most circumstances to deliver good results. The choice of network topology will have an impact not only on reliability but also on the speed of network recovery. The speed of recovery can vary greatly, from 20 ms (e.g., fast ring) to up to several minutes in large networks (e.g., spanning tree root switch failure). This limits the choice of architecture for automated systems because many of these systems are sensitive to network recovery times.

Another important factor is the ease of deployment of the cabling infrastructure. In roadways that are under construction, the network needs to be continuously extended forward to maintain connectivity to the face. This means that during the construction of long roadways many cable joins will be created, which can lead to failure and loss of signal quality.

Choosing a topology will in some cases limit the choice of network hardware because some of the technologies are proprietary. This might limit future vendor choice. In principle, IP-based technologies allow for only a single pathway to be active at any one time; only if this path through the network fails will an alternate path be opened to allow the traffic to travel a different route (fail over). There are some exceptions to this, such as link aggregation, which is usually used to increase bandwidth.

9. BEST PRACTICES AND RECOMMENDATIONS FOR UNDERGROUND MINES

The following section contains topics on communications networks specific to the underground environment, including recommended communications coverage underground; asset and personnel tracking underground, including real-use cases; and installation of equipment underground. The section ends with a case study of LTE implementation at the LaRonde mine by Agnico Eagle®.

9.1 Communications Coverage

Communications coverage systems can be divided into audio, video, data and specialty systems. There are a number of options for each type of communications and will depend on the needs of a specific mine: some options cover certain zones of the mine more easily than others.

9.1.1 Audio Communication Systems

There are several audio communications systems that are suitable for underground mines (Table 6). The systems range from very simple to very complex.

One simple option is a mine phone system. A battery-operated phone is placed at a control location at the surface or entrance into the mine. Additional phones are placed at strategic locations in the mine where work is being done or where personnel will congregate. This technology creates a paging-type system that can be either single zone (all the underground mine) or multizone. Mine phones can be used as a primary communication system but are more commonly installed as a back-up system. Mine phones are simple to install and maintain.

A second common system of underground audio communications is a leaky feeder system, which uses radios and underground antennas. A leaky feeder system allows radios to be used on the surface and within the underground mine in fixed locations. With advances in the technology, this type of system can also be used for limited data communications and specialty controls such as blasting.

A third system is the traditional PBX phone type. PBX systems can be analogue, digital (such as VOIP), or a combination. Fixed phone locations are required for analogue systems. For digital systems, fixed locations are not necessary because an underground wireless network can be used to connect individuals' phones.

9.1.2 Video Communication Systems

Video communication systems are used in monitoring and safety alert systems throughout underground mines (Table 7). Wi-Fi or closed-circuit television (CCTV) are a commonly used system to monitor mining activity. Monitoring devices transmit a visual signal from areas where risk exists for personnel, equipment operation, or interactions

Table 6. Audio Communication Systems and Zones of Coverage in Underground Mines

Zone	PBX phone (analogue)	VOIP (digital)	Mine phone	Leaky feeder
Access area to underground mine	X[1]	X[1]	X[3]	X[2]
Hoist stations	X[1]	X[1]	X[3]	X[2]
Declines	–	–	–	X
Shops	X[1]	X[1]	X[3]	X[2]
Facilities areas (e.g., storage, lunch rooms, fuel storage, electrical rooms)	X[1]	X[1]	X[3]	X[2]
Offices	X	X	–	X[2]
Loading/material storage	–	X	X[3]	X[2]
Long walls	–	–	–	X[2]
Development heading	–	–	X[3]	X[2]
Production/development face	–	–	X[3]	X[2]
Refuge chambers/areas	–	X	X[3]	X[2]
Storage/warehouse	–	X	–	X[2]
Pumping areas	–	–	X[3]	X[2]
Material handling	–	–	–	X[2]

1. Requires analogue or VOIP, not both; 2. Recommended as the primary method of mine communication; 3. Can be used as a primary method of communication, but has limited coverage

Table 7. Video Communication Systems and Zones of Coverage in Underground Mines

Mine area	CCTV	Blinking lights (leaky feeder) for emergency notification	Blinking lights (contactor) for emergency notification
Access area to underground mine	X	X[1]	X[1]
Hoist stations	X	X[1]	X[1]
Declines	–	X[1]	X[1]
Shops	–	X[1]	X[1]
Facilities areas (e.g., storage, lunch rooms, fuel storage, electrical rooms)	–	X[1]	X[1]
Offices	–	X[1]	X[1]
Loading/material storage	X	X[1]	X[1]
Long walls	–	X[1]	X[1]
Development heading	–	X[1]	X[1]
Production/development face	–	X[1]	X[1]
Refuge chambers/areas	–	X[1]	X[1]
Storage/warehouse	–	X[1]	X[1]
Pumping areas	–	X[1]	X[1]
Material handling	X	X[1]	X[1]

1. Blinking lights system can be either leaky feeder or contactor.

between the two. The system can be connected via coaxial cable or digitally. Coaxial connections will be limited by the distance between the device and the monitoring equipment. For digital systems, the bandwidth of the network is the limiting factor.

Safety communications can also be delivered visually using blinking lights systems. This is typically done by connecting the lights in the mine to a contactor that is connected to the surface and would be used to indicate an emergency situation. This type of system is used when "stench gas" systems are not available or not allowed.

9.1.3 Data Communication Systems

Data communication systems are required in a number of locations within the mine (Table 8). When considering data systems, the backbone is the key component. In most

Table 8. Data Communication Systems and Zones of Coverage in Underground Mines

Mine area	Process control (ventilation, dewatering, etc)	IT network	Equipment status IoT (mobile)	Equipment status IoT (fixed)
Access area to underground mine	–	–	X[3]	–
Hoist stations	–	–	–	–
Declines	–	–	X[3]	–
Shops	X[1]	X[2]	X[3]	X[4]
Facilities areas (e.g., storage, lunch rooms, fuel storage, electrical rooms)	X[1]	X[2]	–	–
Offices	X[1]	X[2]	–	–
Loading/material storage	X[1]	X[2]	X[3]	–
Long walls	–	–	X[3]	–
Development heading	–	–	X[3]	–
Production/development face	–	–	X[3]	–
Refuge chambers/areas	–	–	–	–
Storage/warehouse	–	–	–	X[4]
Pumping areas	X[1]	X[2]	–	X[4]
Material handling	X[1]	X[2]	–	X[4]

1. Blinking lights system can be either leaky feeder or contactor.

cases the backbone is some type of fibre optic connection but could also be a leaky feeder system. The number and variety of networks in the mine will inform the quantity of fibre and type of system required.

For process control and equipment status Internet of Things (IoT) systems the amount of data for control and monitoring must to be taken into consideration. The more information that needs to travel between locations and the underground mine the greater the number of fibres required to provide the needed transfer speeds.

9.1.4 Specialty Communication Systems

Specialty systems are used in addition to or as a part of the data network system. They are noted here because they have specific requirements (Table 9). Blasting control, fire detection and annunciation, and emergency communication systems must be installed as per the vendor's requirements and/or any regulatory codes. Access control, geotechnical monitoring, and gas monitoring are additional systems that need to be considered when planning and designing data systems. Asset/personnel tracking requires detailed planning to best achieve the objectives for tracking and networking requirements. In general, the more detailed information that is required for asset and personnel tracking, the greater the required number of access points. Asset tracking is discussed further in Section 9.2.

9.2. Tracking Technologies

An asset tracking system should integrate with existing mine processes to enhance value. It has many benefits, at a minimum assuring productivity; however, it is important to recognize the complexity of implementing an effective system. In lay terms, a tracking system on its own can garner limited value; however, when used in support of mine activities, productivity metrics can be derived and performance improved upon.

Because each mine requires a custom solution, this section is not intended to help in estimating costs; however, it will help answer why a tracking system is so valuable. It will summarize the different technologies and approaches, providing a foundation on which to base the selection of the right tracking system for a specific site.

9.2.1 Asset Location

Asset location tracking systems report on the location of tagged assets or personnel and track their movement throughout areas of the mine in which coverage infrastructure is installed.

The coverage infrastructure should be tailored to meet the requirements of the tracking system. Situational awareness is often associated with asset tracking and helps the end user to determine what is needed from the tracking system. Asset tracking provides the end user with the knowl-

Table 9. Data Communication Systems and Zones of Coverage in Underground Mines

Mine area	Blasting control	Fire systems	Emergency communications	Access control	Geotechnical monitoring	Gas monitoring	Asset/personnel tracking
Access area to underground mine	–	–	X[3]	–	–	–	X[5]
Hoist stations	–	–	X[3]	–	–	–	X[5]
Declines	–	–	X[3]	–	–	–	X[5]
Shops	–	X[2]	X[3]	X[4]	–	–	X[5]
Facilities areas (e.g., storage, lunch rooms, fuel storage, electrical rooms)	–	X[2]	X[3]	–	–	–	X[5]
Offices	–	X[2]	X[3]	–	–	–	X[5]
Loading/material storage	–	–	X[3]	–	–	–	X[5]
Long walls	–	–	X[3]	–	–	–	–
Development heading	X[1]	–	X[3]	–	X[4]	X[4]	X[5]
Production/development face	X[1]	–	X[3]	–	X[4]	X[4]	X[5]
Refuge chambers/areas	–	–	X[3]	–	–	–	–
Storage/warehouse	–	X[2]	X[3]	X	–	–	–
Pumping areas	–	X[2]	X[3]	–	–	–	–
Material handling	–	X[2]	X[3]	–	–	–	–

1. Blasting control has specific requirements for safety; consult manufacturer's requirements for specific systems; 2. Fire systems should report back to a central control area; 3. Several methods of emergency communication are available; refer to Table 15 for recommendations; 4. Connection can be fixed or wireless; if a wireless access point is used, coverage needs to be reviewed; 5. Consideration must first be made to the area where asset or personnel tracking is required; once the areas have been determined, the location of access points can then be planned.

edge needed for situational awareness, which can help with quickly assessing potential problematic situations.

9.2.2 Uses of Tracking Underground

There are a number of reasons to use an asset tracking system in underground mines.

Safety

Worker safety is a critical part of all operations. Having the ability to locate the mine's workforce at any moment is invaluable to ensure workplace safety and in times of site emergency. Tracking can provide information about the location of individual workers and can identify if people are in restricted or unsafe areas. Pinpointing a worker in distress or in an area of danger can save time when every second counts. Accounting for personnel quickly has many advantages. Instead of a manual roll call over the radio—during which the personnel list and locations must be manually produced—the tracking system can instantly output a list of tagged personnel along with their locations. This list can then be quickly verified by radio.

Emergency response

Procedures are developed for high-risk activities performed during underground mining; one critical component of these procedures should be a people tracking system. The information provided by the tracking system will help to locate people during an emergency, for instance if a collapse happens inside the mine. This will enable emergency response teams to focus on impacted areas where people are known to be located, limiting the size of the area for the review and considerably reducing rescue response times.

Tracking

Knowing where the mine's assets—be it human, electrical, or mechanical—are at all times reduces delays. As well as facilitating accountability, ensuring that materials are moved to where they are needed when they are needed will save time and ensure schedules are maintained. Asset tracking is also valuable in locating where mobile equipment has been left at the end of a shift so that the next shift can quickly locate the machines they need to complete their assigned tasks.

Productivity

Using asset tags to monitor the movement of key assets underground can provide analysts with the data they need to optimize processes. For example, assessing travel times and delays can help to recognize opportunities for improvement. Plans can then be developed to optimize procedures to minimize these delays, ultimately reducing costs and positively affecting revenue.

Resource Management

Recognizing where a mine's assets are located and only providing resources to those areas presents an opportunity to reduce costs for resources such as ventilation air, cooling, compressed air, and process water.

Determining which of these factors—safety, asset management, productivity, and resource management—are critical to the operation will help determine the required accuracy needed from the tracking system. This will, in turn, inform the necessary investment required to install a functional tracking system.

9.2.3 Tracking Approach

Two common approaches exist for indoor coverage infrastructure; these are described below:

- **Real-time location system (RTLS):** The location of the tagged asset is determined throughout the area of coverage. The point location is determined through approaches such as "time of flight" or "received signal strength indication". The advantage of RTLS is wider coverage; the disadvantage is that it is ultimately less accurate because of drift. Improved accuracy is achieved with more infrastructure, which adds to the expense of the system.
- **Proximity-based location or chokepoint-based location:** A number of focussed detection areas are installed, in which a detected tag's entry time is recorded accurately. The advantage is that entry into the detection area is accurately recorded; the disadvantage is that these gateways or chokepoints typically provide less than a 10 m radius of coverage at each location. When a tagged asset is between detection areas its true location can only be inferred.

A third approach can be used in an outdoor environment where cellular and satellite tags can be detected by public cellular networks or private satellite networks, respectively. These approaches are not discussed further in this guideline because they are limited to surface mine operations and cannot be applied underground.

Other technologies may be possible, with other capacities. For example, low-frequency tags may provide a larger radius reach underground; however, these are not as typical or common and are not discussed here.

9.2.4 Detection Systems

There are two types of detection systems:

- Passive Tags
  - Chirp when they are excited by a reader
  - The reader is more complex because it requires broadcast capability to excite the passive tag
  - The tag does not have a power supply
  - Limited range: up to 10 m with a fixed reader or up to 5 m with a handheld reader

  - Location accuracy is determined by the strategic location of tag readers in conjunction with the definition of location zones, which provides context to the given location.
  - Less expensive and very simple
- Active Tags
  - Chirp at a defined frequency, from milliseconds to hours (determined by required tracking precision)
  - The tag's chirp is detected by a network of sensing devices
  - The chirp frequency determines the accuracy of location and time of detection data.
  - Powered internally by a battery or externally wired to a power source.
  - Larger range (up to 400 m)
  - Simple sensing devices that simply listen for the tag chirp
  - Sophisticated messaging/signal capabilities

Some tag manufacturers offer hybrid tags, which use active and passive technology and can be used with either active or passive readers. These tags can be used in situations where tracking is required even after the active beaconing or chirping has stopped due to battery power loss.

9.2.5 Base Infrastructure

The mine's underground communication infrastructure will inform what technology approach is used to sense tag locations. Most modern mines have a fibre optic networking backbone, which allows Wi-Fi, LTE, or ultra-wideband technology to be the basis for wireless communications. The wireless system should be chosen with a number of considerations in mind, tracking being only one.

The communication protocol between the tag and the reader can be independent of the protocol used to communicate to the network. Three examples are given below:

- Wi-Fi: The tag communicates to the reader on the 2.4 GHz or 5 GHz band; the reader is usually part of the same Wi-Fi access point used to relay Wi-Fi data to the fibre optic network.
- Bluetooth® low energy (BLE): The tag communicates to the reader with Bluetooth protocol; the reader then communicates to the network over LTE, Wi-Fi, or via hardwire to Ethernet.
- Leaky feeder: The tag communicates to the reader on very high frequency (VHF) or ultra high frequency (UHF) radio frequencies; the reader then communicates to the network via the nearest leaky feeder system amplifier. At the leaky feeder head end a connection is made to the main network.

9.2.6 Location Zones

Maps are an important part of any tracking system. The area of the site shown on a given level map will need to be determined. This will be informed by the selected uses for the system and could be a 100 m square or a 1 km long stretch of drift. The required precision or accuracy of asset location can then be used to determine how far apart the tag readers have to be and their locations can be plotted on the map(s).

Most tracking systems can be programmed to include zones. The size of these zones should be determined in the same way as the size of the map(s). If a small critical zone is required, for example a refuge station or refuelling bay, then sufficient sensing infrastructure will be required to allow accurate location tracking in that limited area. A specific tracking zone can be created for that area, allowing the tracking system's reporting feature to reference that specific zone as a location reference. Zones can be as large as a complete level if desired.

Zones that service a complete level are typical of an RTLS approach; however, with a proximity-based approach, zones are more important and will be smaller. In proximity-based systems, a gateway, chokepoint, or "line in the sand" is created and a specific zone should be associated with this detection point or area. For example, a chokepoint can be installed at a stope access. Once an asset is detected at that chokepoint, its location can be updated with the associated zone name—in this case, the name of that particular stope access.

9.2.7 System Reporting

The tracking system will have the capability to report in at least two ways: by asset and by zone.

Asset Location

This view shows a "breadcrumb trail" of the zones the asset has passed through based on entrance time-stamps. Asset location is useful for determining the timing and path a particular asset has followed over a given period of time.

A variation on this is a list of a number or class of assets, for example, the location of all vehicles at a specific time. This is particularly useful for determining where mobile equipment has been parked at the end of a shift.

Zone Location

This view shows a list of assets that are or were present in the selected location at a specified time, for example, all assets currently in the maintenance shop.

9.2.8 Use Cases

The following examples are included to illustrate actual tracking systems in use underground and their benefits.

Ventilation on Demand

The RTLS tracking mobile equipment was integrated with a smart ventilation control system to provide active airflow setpoints to the ventilation control system. This ensured sufficient ventilation was supplied when people or diesel mobile equipment were present in a given location. The system allowed the main supply fan speed to be optimized, resulting in significant savings.

Truck Fleet Operation Optimization

A chokepoint-based system was used to study and monitor haulage truck movements in an underground mine. Business analysts were able to optimize truck routes to minimize truck hold ups and maximize productivity in a spatially challenging mine.

9.3 Best Practices for Underground Communications Installation

As part of the planning process, an underground site survey should be conducted to:

- Identify and annotate on a mine map the areas of desired coverage
- Identify and annotate on a mine map the locations for power demarcation to access point power supplies
- Identify and annotate on a mine map the locations for existing fibre optic drops/patch panel/existing demarcations
- Identify radio frequency (RF) signal strength and potential sources of interference and attenuation

In target areas, identify the location(s) where communications equipment can be physically mounted with minimal risk of damage, including:

- Access points
- Power supplies
- Cabling
- Antennas

For access points, many devices are mounted using

- Short bolts fastened into the rib or back (depending on rock surface flatness and brittleness)
- Cable ties (zip ties) to mesh screening
- Bolted mounting plates with standoffs for access point mounting

In general, equipment should be mounted on the back (roof) or high enough on the rib (wall) to ensure that it does not protrude in such a way that it will be struck by moving equipment. If the equipment provides status lights that may be used for troubleshooting, consider placement that balances visibility of the lights against risk of damage.

In some cases, mounting the access point in a recessed section of the rib and extending antennas to the centre of drift using low-loss cable provides both ease of access and minimal risk of damage. Look for these during the site survey.

Similarly, cabling should be strung and secured at regular distances as specified by the individual supplier's specifications (e.g., every 3 m using cable ties or cable hooks, fastened to the back or rib or to existing messenger wire).

It is recommended that cabling not be tied to other infrastructure such as high voltage cabling, water, and air lines because maintenance to these services may result in the need to remove and relocate communications cabling.

When calculating cabling distances during the site survey, it is recommended to add 10–15% additional cabling to account for variations in actual installations due to placement of cable relative to other infrastructure, drip loops, and extra length needed for repairs and re-terminations. After connecting cabling to the AP, wrap the cable end and connector with self-amalgamating tape (Figure 17) to add further protection against water ingress.

Wi-Fi antennas can be mounted or extended from APs using low-loss cable and mounted in the centre of the drift. Consideration should be given to how low antennas hang to avoid displacement and/or damage from moving equipment.

Antennas should be fastened in such a way that the directionality of the antenna does not change due to air flow when auxiliary fans are used. For example, avoid using chains hung from the wire mesh used for ground support. Consider using fixed brackets to secure antennas in place, thereby minimizing the loss of communication from antenna movement.

Avoid installing antennas near other sources of RF emissions such as adjacent fan starters or motor drives. Potential sources of RF noise should be identified during the site survey.

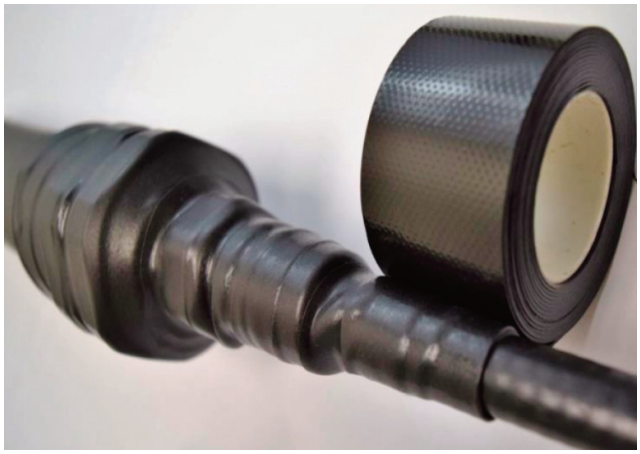


Figure 17. Self-amalgamating Tape Protects Cable Infrastructure Against Water Ingress.

For Wi-Fi deployments, careful consideration should be given to antenna types and the desired directionally of signal propagation. Three common antenna types used in underground mining tunnels are:

- Omnidirectional: directs RF energy in a spherical direction around the antenna
- Directional: directs the RF energy in a specific direction (varying by radiating pattern of the antenna)
- Yagi: directs RF energy in a very narrow direction and is typically used for greater range

Maintain a network topology map of all devices and the system layout and endeavour to maintain and update it whenever devices are removed, replaced, or added. In addition, maintain a device registry for all parts of the communication network that includes

- Device label, such as AP-3702-5300-OREPASS
- Device make, model, and date of deployment
- Maintenance records, including patch and upgrade records
- Serial number(s)
- Number and type of antennas
- Media access control (MAC) address of each radio
- IP address(es)
- Location of device on the network topology map

9.4 Case Study: Implementation of LTE at LaRonde Mine

The following is based on a September 20, 2018, interview with Sylvain Bernier of Agnico Eagle.

The LaRonde mine is a major gold-producing underground mine in northwest Quebec, Canada, with more than 240 km of underground workings. The orebody is getting deeper and further from shafts, which has decreased equipment and worker productivity due to increased travelling time. The depth and extensive galleries call for critical management of ventilation and cooling to meet the increased heat at depth. The extent of equipment and staffing calls for a robust and flexible communications network.

Current main mine communications consist of leaky feeder, VHF radio, fibre optic cabling, and production face Wi-Fi. With 40 operational levels, these technologies provide limited coverage (at most 75% at secondary infrastructures), have middling signal quality and reliability, and are difficult to maintain. This is not necessarily a problem, but with the need for increased automation, Wi-Fi was not considered a feasible solution. Wi-Fi installations require individually configured and powered access points positioned every 100 m. These points are taken to the production face, then removed for re-installation elsewhere once the production face moves. This does not offer as flexible a network as is required for automated production work. In addition, the complexity of the Wi-Fi access points requires substantial time for installation and maintenance. As a result, this technology can no longer be supported.

LaRonde is developing the LZ5 ramp approximately 4 km from the main site. This ramp is accessed from an open pit and has a limited lifespan of 2018 to approximately 2026 and a projected production of 401,000 oz of gold. As a greenfield site, LZ5 was considered a perfect test bed for new LTE communications technology. At LZ5, fibre optic cable runs between levels to the surface and connects to the LTE broadcast base unit (BBU) that communicates with PLCs and servers. At the beginning of each level, an LTE remote radio unit (RRU) interfaces between the fibre optic backbone and the repeater antennas on the level. The antennas are spaced every 50 m and connected by coaxial cable in series back to the RRU. Only the single RRU requires power on each level; the individual antennas do not require power. The 50 m long coaxial cable lengths and splitters are pre-assembled by the supplier.

Neither the RRUs nor the antennas require any configuration once installed; all configuration occurs at the BBU on the surface. This results in underground components that are effectively "plug-and-play"; if an LTE antenna or cable is damaged, anybody can replace the damaged item with a standard part in stock from the warehouse. This successfully moves the complexity of the installation from underground to the surface, where more resources are available.

The LTE project at LZ5 has so far been successful. The most challenging part of the project includes ensuring proper communication between the BBU and servers, although this is largely the same as with Wi-Fi because both use IP standards. Convincing equipment suppliers to provide LTE radios on the equipment (instead of Wi-Fi) was an additional unforeseen challenge. Neither of these issues has resulted in cost increases. Overall, the cost-per-metre (including RRUs, cables, and antennas) for LTE installation is lower than for Wi-Fi (approximately C$30/m average vs. more than C$50/m for Wi-Fi). The server core and licensing for LTE is higher than for Wi-Fi; however, the overall lifecycle cost of the integrated LTE network (for high performance data and voice capacity) with much easier configuration, installation, and maintenance is anticipated to be much lower than for Wi-Fi. Additionally, LTE provides better cybersecurity.

Operators are also enthusiastic about using mobile phones for their applications (broadcast and 1:1 communications, push-to-talk, tracking, text messaging, and photos at the face). The use of mostly familiar mobile devices is welcome, audio quality is high, and no one is asking to return to radio standards.

Although LZ5 is a greenfield application of LTE, LaRonde has plans to implement LTE in their older workings. This will occur gradually, with LTE being installed in new production zones continuously until the older zones and their older technologies are no longer in play. LaRonde also has vision for LaRonde 4.0, which involves implementing new technologies for further capture of deep and low-grade resources. This will also improve working conditions for the workforce.

10. NETWORK SECURITY FOR UNDERGROUND MINING OPERATIONS

This section consists of a general discussion of security risks due to unauthorized physical and data level access, how and where these breaches can occur, and the unique challenges surrounding modern technologies such as wireless and IoT. A discussion of networks segmentation to facilitate security completes the section.

10.1 Operational Technology (OT) Security

10.1.1 IT security considerations for underground mining operation

IT security can be divided into two major branches: physical access and data-level access. Both require constant attention and are of equal importance in protecting the operation from loss of production and sensitive data. Security breaches can be further separated into intentional and unintentional. A person might maliciously cut a cable or they could be unaware that the USB device they are using contains software (e.g., a Trojan) that opens a backdoor into the network, granting unauthorized access.

10.1.2 Physical Access Protection

Physical access protection mitigates the risk of an unauthorized person physically accessing infrastructure; the required level of protection varies greatly and should be evaluated by assessing the possible impact of loss of safety for personnel and production. Wherever possible, protection should be applied to the system as a whole and include items such as the power infrastructure supplying the IT systems and data backbones connecting the mine to the outside world.

Restricting access to the infrastructure can be achieved in different ways and a common-sense approach is required; there must be a trade-off between ease of legitimate access and level of protection. For example, mounting a wireless access point on a 15 m mast or the back (roof) of a roadway makes for good physical access protection: however, the location makes servicing the equipment difficult.

Similarly, locating a server running an automation production system in a well-protected server room on the surface makes good sense from the standpoint of protection and serviceability; however, this commonly introduces long cable runs, rendering the system vulnerable to malicious and accidental cable damage. Depending on the situation, it might be justified to locate the server in a specially built communication enclosure near the production site, despite it being more difficult to access or more costly to construct.

Physical protection needs can differ greatly depending on a number of factors. For example, theft of cable for copper content or removal of batteries from mobile devices is common in third world countries; however, these are rare occurrences in developed countries. In developed countries, the greater risk is likely to be a disgruntled employee gaining unauthorized access to the network and causing damage.

A formal assessment of the risk to the operation will justify the need for the level of protection required. Table 10 is a basic guide to assessing the risk to infrastructure and the impact to the operation. The table is a guide only and should be expanded to site-specific risks.

10.1.3 Data Level Access

Protecting modern IP data networks is an ever-evolving task and requires highly trained personnel and specialized technology. Large organizations have specialized IT security teams constantly monitoring for possible security breaches and updating the network with the latest software and equipment to prevent unauthorized access.

The effort a hacker will invest to penetrate the security of a network is usually directly related to the value that can be gained. For example, the production cost of a commodity for a mine or mining company may be a very valuable piece of information during the negotiation of long-term supply contracts to other companies or even governments, making it a high-value target for internal and external security breaches. The effort invested to penetrate these networks will be high, requiring equally strong counterprotection measures.

10.1.4 Internal and External Risk

Commonly, the risk of external network breaches is seen as a major threat, but statistically the risk of an internal breach is far greater. A disgruntled or corrupt employee with the right skillset and access level can cause significant damage to an organization. Additionally, these breaches often go undetected for years or are never discovered because it is difficult to ascertain if the access to data is a breach or part of day-to-day IT maintenance tasks.

The need for networks to be connected to the wider organization and the outside world requires access to

Table 10. Sample Guidelines for Risk Assessment of Security of Physical Network

Type of infrastructure	Level of risk to safety	Level of risk to production	Difficulty to implement	Impact on serviceability	Protection to implement
Uninterruptible power supply (UPS) server farm and voice communications	Extreme	Extreme	Medium	Low	- Fully enclosed, lockable (key and or unique identifier [UID] card) - Encapsulated external cable infrastructure communications - Monitoring - Movement sensor - Alarmed
On-level access network switch	Medium	Medium	Low	Medium	- Locked cabinet - Internal UPS - Accessible cable in solid cond
Fibre distribution cable underground core network	Extreme	Extreme	High	Low	- Limit physical access (e.g., borehole, multiple redundant path, solid conduit, fail-over monitored)

broader IT networks, making it increasingly difficult to protect the network. With the increasing use of software and automated equipment, third parties need remote access to the network to maintain, troubleshoot, and update software and equipment. The risk of a third party accessing the network needs to be evaluated on a case-by-case basis. The process of granting and revoking third party and/or employee access to the network can be time consuming and complex.

10.1.5 Wireless Networks

Wireless technologies are delivering increasing capability in mine operations networks and the uptake of these technologies is rapid and growing. The mobility of this technology makes it very attractive. Connecting mobile production equipment such as drill rigs to a wireless network has become the default; tracking of personnel and wireless voice communication is very common. The removal of the need to be physically connected to the network to gain access is a significant convenience and the miniaturization of devices that can access the wireless network, driven by the mobile phone, is a significant achievement; however, these advantages also create a long list of security problems, such as susceptibility to hacking, the need for secure passwords and encryption, the possibility of malicious software being inadvertently embedded in the network, and security holes being exposed simply due to ignorance of new threats or the lack of regular software updating, among others.

10.1.6 Internet of Things (IoT) and Telemetry

In recent times, network breaches have occurred that involved traditional telecommunication infrastructure or connected telemetry devices (IoT). These relatively new IoT technologies are changing the way underground mine networks are managed and controlled. The uptake is still relatively slow; however, there are clear indications that there will be explosive growth in this area. From a security standpoint, this is a new frontier. Most of these devices have embedded network protocols that provide excellent security measures; however, there are few IT professionals who understand these new technologies because they are not based on the well-understood traditional IP system.

10.2 Malicious Software

Malicious software and viruses are a real risk to any network. Not only can this type of software destroy valuable data, it can render networks inoperative for long periods. Once a virus has penetrated the security of a network it can be difficult to eradicate because it can disguise itself and/or lay dormant for a long time. Some of these malicious tools can facilitate the access to the network from the inside by effectively opening a "back door". There are many ways for unauthorized software to get into the network; email, USB devices, mobile computers, and mobile phones connected to the network are the most common paths of infection.

10.3 Segmentation to Facilitate Network Security

Network security can be facilitated by segmentation, the separation of the network into smaller subnetworks, with differing purposes, physical attributes, and security needs (Figure 18). Segmentation can be accomplished with logical separation, where different systems communicate on the same physical layer (such as an Ethernet LAN) and firewalls restrict the types of communications; or physical, where communication occurs through different physical channels (Mahan et al., 2011). Figure 18 schematically represents how a network can be segmented.

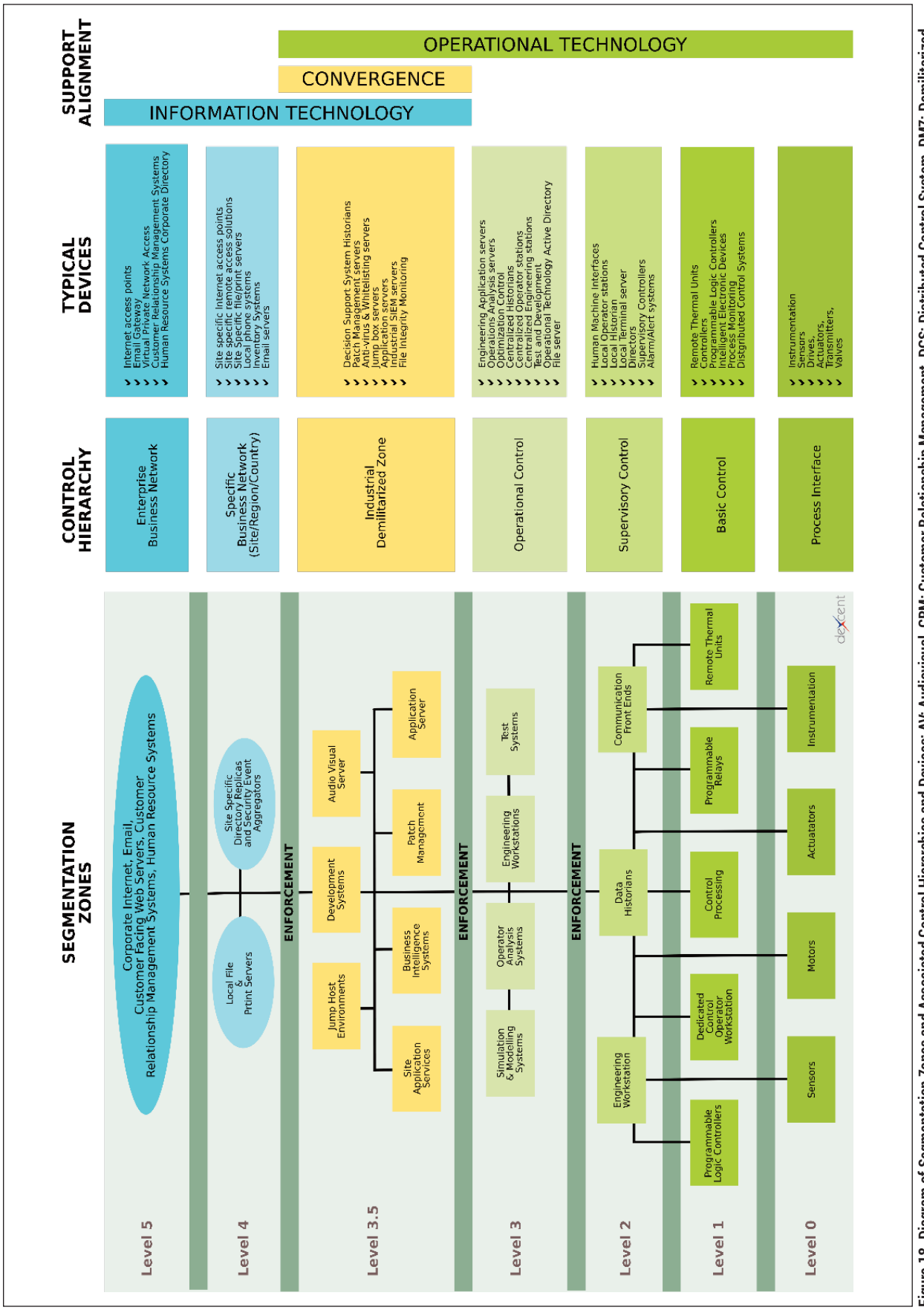


Figure 18. Diagram of Segmentation Zones and Associated Control Hierarchies and Devices; AV: Audiovisual, CRM: Customer Relationship Management, DCS: Distributed Control System, DMZ: Demilitarized Zone, DSS: Decision Support System, HR: Human Resources, OT: Operational Technology, PLC: Programmable Logic Controller, RTU: Remote Terminal Unit, SCADA: Supervisory Control and Data Acquisition, VPM: Virtual Private Network.

In most mines, as in most businesses, there is a need to access the Internet (level 5, enterprise business network) for email, customer-facing web servers, cloud services, virtual private networks (VPNs), and other applications. Workstations at this tier should be protected by a firewall and router at the Internet access point as would be typical in a business IT environment.

Level 4 (specific business network) concerns local file and print servers, and site-specific data. Devices at this level can have significantly restricted Internet access, perhaps to a limited whitelist or only remote VPN targets within the same company. Devices from level 3.5 likely require access to some services at this level.

The industrial demilitarized zone (DMZ) at level 3.5 is where IT and operations converge. Users or systems working at this level likely need access to the Internet for research, planning, and communication; they also require access to lower tiers of operational data. For example, antivirus servers must be able to scan devices at level 3 (and perhaps below) but also require updated virus definitions from the Internet, so they necessarily exist at this level.

A major segmentation occurs at level 3: Devices at this level may interact with devices at level 3.5, but everything at and below level 3 should not have access to the Internet. When software updates are required below level 3.5 or data are reported elsewhere in the company, the transfer must be mediated through the industrial DMZ. Level 3 necessitates isolation from the company's Active Directory (or user credential database), so a separate credential database must be established, and site-specific login credentials issued. Operational analysis is performed at this level, based on data from lower levels.

Levels 1 and 2, the workstations and electronics that read sensors and control actuators, must have the highest level of physical security because there is potential to do real damage to the mine's operations if security is compromised. It is from here that a malicious actor could bypass safety mechanisms or drive equipment beyond safe limits. Workstations that control these functions ideally should be air-gapped (i.e., isolated from the LAN) and be located in a physically secure control room (e.g., under lock and key, with security cameras). Precautions should be taken when foreign electronic equipment such as USB drives or laptops are brought in contact with these workstations since sophisticated attacks against even military air-gapped systems have succeeded. The Stuxnet virus (Falliere, Murchu, & Chien, 2011) is a prime example.

In level 0, Figure 18 shows sensors, motors, actuators, and instrumentation. In many plants these devices would be on a secure "factory floor", physically isolated from other systems. In a mine, these devices are necessarily distributed throughout the mine, and in some cases, exposed in a way that makes physical security impossible; however, it is very difficult to orchestrate an attack on a mine from level 0 without having access to level 1. Mine architects should be aware of the vulnerability at this level and plan accordingly.

10.4 Network Security—Conclusions

Network security is an ever-evolving topic requiring constant focus and maintenance. Only a solid security framework can protect a network. Highly skilled IT professionals are required to maintain and update the various tools that protect the physical network and its data. Large organizations should have an in-house team that can implement and constantly maintain the security framework. Mines that do not have access to such a team are strongly advised to subcontract these tasks to a reputable company that specializes in IT security. In some instances, it might be possible to physically isolate networks (air gap) from any connectivity with the outside world. This is not uncommon in fully automated production systems. Outside access to such networks is only granted at arranged times and under strict conditions. When implementing new technologies such as IoT networks, it is advisable to ensure that the contractors implementing these new technologies collaborate with the contracted security specialist to minimize risk. Regular security audits by an independent third party are a good measure to ensure that the in-house team or contractor is performing as expected. Security, not unlike safety, is every employee's business and employees should be encouraged to be vigilant and report unusual activity.

Despite all efforts, it is not a question of if an operation will experience an attack, but a question of when an attack will occur. In addition to taking steps to prevent security attacks, organizations should have a disaster recovery plan in place that addresses the identification of a network security attack, the steps required to halt the attack, and a tested plan to restore the network after the attack. The objective is to recognize what is happening, minimize the impact, and restore operations as quickly as possible.

11. CONTROL ROOMS AND REMOTE MANAGEMENT

This section defines the terms used to describe remote operations, discusses benchmarking requirements for different types of remote operations, and explores control room and remote operations station designs and ergonomics.

11.1 Definitions for Remote Operations

The following terms are defined with respect to their use in the context of underground mining networks and remote operations.

- **Control:** The manipulation of a piece of equipment, resource, procedure, or process to produce a desired outcome.
- **Local:** The physical environment that makes up the operational site. Within the context of underground mining networks, local is defined as the area within the boundaries encompassed by the site local area network (LAN). This is typically limited to the geographical footprint of the mining operation, in which the network latency is within the direct control of the owner.
- **Local control:** The act of manipulating or otherwise altering the operational action and outcome of a resource, asset, process, or procedure from a location that is removed from the physical location of the target of the control action but within the boundaries of the LAN. Local control requires two-way (backhaul) communication channels.
- **Local monitoring:** The act of observing operational actions and outcomes from a location that is removed from the physical location of the target of observation but within the boundaries of the LAN. Local monitoring requires a one-way communication channel.
- **Remote:** The area beyond the boundaries of the LAN or the source site's geographic boundaries. Within the context of underground mining networks, a remote network connection can include connection to, or consolidation of, data at the regional, national, continental, or global level.
- **Monitoring:** The observation of assets, processes, or procedures using communication channels to relay images or electronic data from a source to an observer. The observer may be a human operator or an automated process.
- **Process:** A piece of work that has a defined start and finish and consists of a set of actions or steps that result in a desired outcome.
- **Remote control:** The act of controlling the operational actions and outcomes from a location that is removed from the physical location of the target of the control action and beyond the boundaries of the LAN. Remote control requires a two-way (backhaul) communication channel.
- **Remote monitoring:** The act of observing operational actions and outcomes from a location that is removed from the physical location of the target of observation and beyond the boundaries of the LAN. Remote monitoring requires a one-way communication channel.

11.2 Remote Operations and Benchmarking

The determination of whether remote control can be used in an operational environment must be based on the possible response time to a changing event (network latency); the required response time or window within which to effect a change (criticality); and the resulting outcome if the change is not enacted within the required time (risk). The physical distance between the source and the controller cannot be used as the single basis for overall effectiveness because the remote control of operations relies on the speed of communication. Distance is only one of several contributing factors to the overall speed of data transfer.

When assessing latency for the purpose of remote operational control it is important to remember that, to be realistic or actionable, network latency determinations must include the whole network. Measurement should take into consideration the entire round trip, from the asset's transmission of data to the controllers' receipt followed by the receipt by the asset of a return instruction. This calculation would typically not include the controller assessment cycle, nor should it include the time it takes the asset to enact the change instruction.

The determination of what operations or processes can be remotely managed requires an evaluation that includes a process assessment, risk assessment, and zone classification.

11.3 Monitoring

For system standards purposes, one should consider all transactions as having a return communication requirement. Although control requirements imply a return communication, monitoring functions may not explicitly require it. There are two fundamental types of monitoring: business and operational.

Business monitoring needs draw data from the source for use in business applications and functions where it typically serves strategic, financial, and planning purposes. Business monitoring should have no need for return communication directly to the site operations. If the mine operator discovers that the business monitoring does have a need to directly change operational parameters, they should take this as an indicator that that process should not reside with the business monitoring division.

Operational monitoring, on the other hand, always has a return communication expectation. The method of communication can vary from a data transmission (e.g., text or email) to a telephone call or physical action.

The primary difference between an operational monitoring and an operational control function is the response time

required and the function of the observer. Operational control generally requires the observer to be actively engaged with and directly manipulating a controllable device. Operational monitoring generally requires an observation and an indirect response. The response can be a notation on a log or it can require an engineer to call an operator with instructions to implement a change. In either case, operational control and monitoring both require some type of response.

Given that a response is required, the question becomes: How long is an acceptable timeframe for the data to get to the observer, for the observer to process the information, for the observer to formulate and enter a response, and for the response to get back to the source location? Depending on the criticality, the acceptable response time might be counted in milliseconds, minutes, or hours.

Ultimately, the decision of how far away remote monitoring or control can be situated is a function of the response time required, which is in turn dictated by the criticality of the function. Risk management methodology should be applied to determine the required parameters.

11.4 Process Risk Assessment (Example)

Mine design requires consideration of the response time requirements for all aspects of the site and the operation. The business must conduct a process risk assessment to determine the acceptable response parameters for each process that requires remote observation. An over-arching risk assessment question should be: What happens if the network goes down? Table 11 shows an example of acceptable response times for a series of mine processes determined through process risk assessment. The maximum zone allowed is determined at a later point.

11.5 Zone Classification (Examples)

Once the required response times have been determined, the processes can be grouped together within bands of acceptable response times, creating a series of control zones. These zones could range, for example, from "critical response – observer required within visual range" to "low priority response – greater than one hour".

Zone classifications can be simply generated using a table such as the example in Table 12. The response times and zones in Table 12 are for illustration purposes; actual required response times, and the zones required, should be developed by mine operators using process risk assessment.

Alternatively, a table similar to Table 13 can be used to more accurately define the physical zones required. This approach can be useful to define zones that have alternate response channels. For example, a process may send operational data to the remote destination with an expectation of a return response via email. In these instances, the time to transmit data is measured in milliseconds, whereas the required response may be measured in minutes. The overall round trip should be considered in determining the remote zones.

11.6 Process Zone Matrix

Once they are classified, the zone are associated back to the processes to define which processes can be addressed in each zone. This information can then be used to determine the hardware, software, and network needs of each remote control location (Table 14).

Table 11. Sample Required Response Times

Process	Response time required (s)	Maximum zone allowed
Drill control – critical stop	< 1	
Primary conveyor stop	< 5	
Primary crushers stop	< 10	
Semi-autogenous grinding (SAG) mill critical stop	< 5	
Primary crusher conveyor speed	> 30	
SAG mill feed control	> 30	

Table 12. Sample Table of Physical Zone Classifications Based on Process Risk Assessment

Physical Zone Classifications		
Response time (s)	**Zone #**	**Zone description (determined by benchmarking)**
< 1	0	On site, at asset
< 5	1	Plant control centre
≤ 10	2	Regional control hub
> 10	3	National control centre
≤ 30	4	Global centre

Table 13. Sample Table for Zone Determination

Zone determination				
	Network transfer time (ms)			
Physical location	**Location to remote**	**Remote to location**	**Round trip**	**Zone classification**
Face – drill				
Crushers				
SAG mill				

Table 14. Process Zone Matrix

Process	Response time required (s)	Maximum zone allowed
Drill control – critical stop	< 1	0
Primary conveyor stop	< 5	1
Primary crushers stop	< 10	2
SAG mill critical stop	< 5	3
Primary crusher conveyor speed	> 30	4
SAG mill feed control	> 30	4

Testing is required to determine where these zones are located with respect to the source. Tests should investigate the time it takes for data to travel from the point of origin though the network and all in-line network devices to the proposed end observation point. A similar test would be required for return or backhaul communication. In addition to testing the communication speed, bandwidth must be considered to ensure adequate data volumes can be transmitted.

Depending on the location of the source and observer positions, mine operations may need to consider regional control hubs connected to larger centres to meet the required process response times.

A note of caution for time series data historian users: If a portion of the network traffic requires the transmission of time series data from historian databases, benchmark testing should consider the additional loads placed on the network if the flow of streaming data is interrupted downstream of the source. In the event of a network outage, most historian database systems will buffer data at the source. When the network is re-established, the buffered data is uploaded. The volume of data can be very high in these instances and can impact all network systems.

Although the amount of data buffered depends on the vendor, hardware, and a variety of other factors, there does seem to be a de facto standard of 72 h of data that is retained at source. For instance, a single haul truck can generate roughly 200 data points every 3 s. Over the course of a 72 h network outage, the unit will need to upload more than 25 million data points when the connection is re-established. This can have a significant impact on all remote operational functions, especially if multiple assets are impacted by the outage.

11.7 Control Room and Remote Workstation Design

In the age of digitization in the mining industry, there is more reliance and focus on the remote operation of machinery from a control room, whether remotely or centrally located. Control room ergonomics is an important consideration, not only for the safety of operation, but also for worker comfort, efficiency, and productivity. The examples that follow illustrate proper execution of ergonomics and areas for improvement, which can be incorporated into a "best practices" guideline for mine site control rooms and remote workstations.

There are many guides on how to properly lay out and implement a control room that consider ergonomics. The examples that follow align with and build upon findings in Mast (2007) and Lundmark (n.d.), two papers that outline specific criteria for ergonomics when designing a control room.

The mine owner and/or system designer should consider these factors when implementing a remote control system as part of their "change management" process to facilitate effective integration of these technologies into their operation.

11.7.1 Remote Workstations

Figure 19 shows an individual using a remote workstation. The following attributes of the station are examples of good ergonomics:

- The station is designed so that the controls feel like the system they operate but are not exactly the same. This gives the operator some familiarity compared to operating the device directly while also keeping the focus on the environment and preventing complacency (Wickens et al., 2004, p. 117–119).
- The multiple display screens are arranged sequentially in order of use, which facilitates the flow of information. This arrangement could be improved with the use of one large screen with a simple, organized layout because when multiple screens are used, the attention is diverted from one to the next instead of viewing the

Figure 19. Remote Operation Station with One Operator

entire system continuously (Wickens et al., p. 198–201).

- The use of armrests supports the operator while seated.

This example also demonstrates several opportunities where improvements could be made:

- Consideration of the location of the joystick and other input devices with respect to the operator's body position, and provisions for adjustability of the operating station would reduce body strain caused by unnatural joint positions and allow each operator to find the perfect fit regardless of their proportions (Wickens et al., 2004, p. 267–268, 293–295, 387–390).
- The keyboard location suggests that there is no designated space to use it. A stand or tray should be incorporated that takes into consideration the frequency of use, proper height for operation, and the ability of the operator to use the rest of the station (Wickens et al., 2004, p. 267–268, 293–295, 387–390).
- The contrast between on-screen cues and the background should be maximized and glare should be minimized to ensure that the operator can manipulate the machine safely and accurately (Wickens et al., 2004, p. 69–72, 363–365).
- It is unclear how the operator enters and exits the workstation and whether it is safe, clear path (Wickens et al., 2004, p. 363–365).
- The workstation appears to be cramped (Wickens et al., 2004, p. 363–365).

It is also important to consider the location of safety equipment: the safety box should be prominently located in the station and the radio should be within easy reach of the operator (Wickens et al., 2004, p. 69–72, 285–287, 292–295, 398).

Figure 20 is an example of a multi-person remote workstation. The following attributes of the station are examples of good ergonomics:

- Feet and arm rests and an appropriately reclined backrest (110–120°) minimize static loading of muscles and body strain.
- Multiple workstations allow controls to be passed off to a co-worker during breaks.
- Display screens are properly illuminated and focused, and brightness can be adjusted to suit the user.
- There is minimal clutter; all relevant information is displayed on one screen.
- The station is designed so that the controls feel like the system they operate but are not exactly the same. This gives the operator some familiarity compared to operating the device directly while also keeping the focus on the environment and preventing complacency (Wickens et al., 2004, p. 117–119).

It is noted that there is a risk with multi-person operation stations that the attention of an operator could be impacted by the close presence of other operator stations.

11.7.2 Control Rooms

Figure 21 shows an individual using a control room. The following attributes visible in this image are examples of good ergonomics:

- The room is well lit, with a window and natural light available.
- Visibility outside the workstation is provided, possibly including direct line of sight to work area and personnel.
- Good proximity to communication devices: telephone and radio are right on the desk.

Figure 20. Multi-person Remote Operation Station

Figure 21. Control Room with One Operator

This example also demonstrates several opportunities where improvements could be made:

- Displays are not all well positioned; the display on the left requires that the user rotate their body to view it. The displays are also placed a different heights.
- The keyboard is poorly placed and will result in upper body strain with continued use in this position.
- The desk chair does not adjust to allow the user to more easily reach the keyboard.
- The radio control box should ideally be placed closer so that the channel can be changed with ease.

Figure 22 shows a multi-user control room. The following attributes visible in this image are examples of good ergonomics:

- The physical environment is well lit and tidy with lots of room to work.
- Workstation ergonomics are good (chair height, keyboard placement).
- Displays use an appropriate font size, with larger displays at a distance using larger font for easy visibility.

This example also demonstrates several opportunities where improvements could be made:

- The screens appear to be quite bright with significant white; this can lead to eye fatigue.
- The variety of chairs allows for some adjustability; however, consistency is also important. It is important to take into consideration the preferences of the mine controllers and what is comfortable for them; many chairs on the market allow for significant customizability, so spending more up front for these units will allow for simplicity of ordering and consistency.

Figure 22. Multi-user Control Room

12. RESOURCES, REFERENCES, AND RECOMMENDED READING

Ambra Solutions Inc. (2018). Ambra's products and solutions; Unpublished PowerPoint presentation.

Australian Communications and Media Authority (ACMA) (2018). The ACMA overview. Retrieved from https://www.acma.gov.au/theACMA/About/Corporate/Structure-and-contacts/the-acma-overview-acma

Australian Government (1992). Radiocommunications Act 1992, Section 162. Retrieved from http://www7.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/ra1992218/s162.html

Australian Government (1997). Telecommunications Act 1997, Section 376. Retrieved from http://www8.austlii.edu.au/cgi-bin/viewdoc/au/legis/cth/consol_act/ta1997214/s376.html

Australian Government (2018). Australia Broadcasting Services Act 1992, Section 9A. Federal Register of Legislation. Retrieved from https://www.legislation.gov.au/Details/C2005C00400

Australian/New Zealand Standard (2000). AS/NZS 2802:2000: Electric cables–Reeling and trailing for mining and general use (other than underground coal mining). Retrieved from https://www.standards.org.au/standards-catalogue/sa-snz/mining/el-023/as-slash-nzs—2802-2000

Australian/New Zealand Standard (2004). AS/NZS 3085.1:2004 (R2016): Telecommunications installations—Administration of communications cabling systems. Retrieved from https://infostore.saiglobal.com/en-us/standards/as-nzs-3085-1-2004-r2016—117105_SAIG_AS_AS_244984/

Australian/New Zealand Standard (2009a). AS/NZS 4240.1:2009: Remote control systems for mining equipment: Design, construction, testing, installation and commissioning. Retrieved from https://infostore.saiglobal.com/en-us/Standards/Product-Details-129903_SAIG_AS_AS_275008/?ProductID=129903_SAIG_AS_AS_275008

Australian/New Zealand Standard (2009b). AS/NZS 4240.2:2009: Remote control systems for mining equipment. Retrieved from https://www.standards.org.au/standards-catalogue/sa-snz/mining/el-023/as-slash-nzs—4240-dot-1-2009

Australian/New Zealand Standard (2014). AS/NZS 2967:2014: Optical fibre communication cabling systems safety. Retrieved from https://infostore.saiglobal.com/en-us/standards/as-nzs-2967-2014-119660_SAIG_AS_AS_250753/

Communications Alliance Ltd. (2013). Australian Standard AS/CA S009:2013: Installation requirements for customer cabling (wiring rules). Retrieved from http://www.commsalliance.com.au/__data/assets/pdf_file/0017/39203/S009_2013.pdf

Communications Regulatory Commission of Mongolia (CRC) (2018). Website. Retrieved from http://www.crc.gov.mn/en

Communications Regulatory Commission of Mongolia (1999). Law of Mongolia on Radio Wave. Retrieved from http://www.crc.gov.mn/en/k/x5

Communications Regulatory Commissions of Mongolia (2001). Law of Mongolia on Communications. Retrieved from http://www.crc.gov.mn/en/k/xd

Communications Regulatory Commission of Mongolia (2013). 2013-26: Regulation Information and Communication Network of Mongolia. Retrieved from http://www.crc.gov.mn/en/k/2lW

Communications Regulatory Commission of Mongolia (2016a). Directions, terms and requirements of procedures and regulations approved by the CRC. Retrieved from http://www.crc.gov.mn/en/k/1b/1l

Communications Regulatory Commission of Mongolia (2016b). Mongolian communications standards. Retrieved from http://www.crc.gov.mn/en/k/1h/1r

El Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL) (2018). Website. Retrieved from https://www.osiptel.gob.pe/

Falliere, Murchu, & Chien (2011). W32.Stuxnet Dossier. Symantec Security Response. Retrieved from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Federal Communications Commission (FCC) (2018). Website. Retrieved from https://www.fcc.gov/

General Agency for Specialized Investigation (GASI) (2016). Website. Retrieved from http://inspection.gov.mn/

Ghana National Communications Authority (NCA) (2018). Website. Retrieved from https://www.nca.org.gh/

Ghana Civil Aviation Authority (GCAA) (2016). Website. Retrieved from http://www.gcaa.com.gh

Ghana Environment Protection Agency (EPA) (2018). Website. Retrieved from http://www.epa.gov.gh/epa/

Ghana Ministry of Lands and Natural Resources (2016). Minerals Commission (MINCOM). Retrieved from http://www.mlnr.gov.gh/index.php/agencies/minerals-commission

Global Mining Guidelines Group (2017a). Underground mine communications infrastructure guidelines, part I: Positioning and needs analysis (Standard No. 20161117_Mine Communications Infrastructure I-GMG-UMuci-v.05-r1). Retrieved from https://gmggroup.org/wp-content/uploads/2018/06/Mine-Communications-Guideline-I-REV-2018.pdf

Global Mining Guidelines Group (2017b). Underground mine communications infrastructure guidelines, part II Scenarios and applications (Standard No. 20161116_Mine Communications Infrastructure II-GMG-UMUCI-v.08r2). Retrieved from https://gmggroup.org/wp-content/uploads/2018/06/Mine-Communications-Guideline-II-REV-2018.pdf

Government of Western Australia (2013). Electricity Act 1945. Retrieved from https://www.legislation.wa.gov.au/legislation/prod/filestore.nsf/FileURL/mrdoc_25559.pdf/$FILE/Electricity%20Act%201945%20-%20%5B08-a0-03%5D.pdf?OpenElement

Government of Western Australia (2015). WA Electrical Requirements. Department of Mines, Industry Regulation and Safety. Retrieved from https://www.commerce.wa.gov.au/publications/wa-electrical-requirements-waer

Government of Western Australia (2017). Mines Safety and Inspection Regulations 1995, Version 06-d0-05. Retrieved from https://www.legislation.wa.gov.au/legislation/prod/filestore.nsf/FileURL/mrdoc_29691.pdf/$FILE/Mines%20Safety%20and%20Inspection%20Regulations%201995%20-%20%5B06-d0-05%5D.pdf?OpenElement

Government of Western Australia (2018a). Occupational Safety and Health Act 1984. Department of Justice. Retrieved from http://www8.austlii.edu.au/cgi-bin/viewdb/au/legis/wa/consol_act/osaha1984273/

Government of Western Australia (2018b). Occupational Safety and Health Regulations 1996, Version 10-e0-00. Department of Justice. https://www.slp.wa.gov.au/pco/prod/filestore.nsf/FileURL/mrdoc_41104.pdf/$FILE/Occupational%20Safety%20and%20Health%20Regulations%201996%20-%20%5B10-e0-00%5D.pdf?OpenElement

Government of Western Australia (2018c). Mines Safety and Inspection Act 1994, Version 06-c0-00. https://www.legislation.wa.gov.au/legislation/prod/filestore.nsf/FileURL/mrdoc_41380.pdf/$FILE/Mines%20Safety%20And%20Inspection%20Act%201994%20-%20%5B06-c0-00%5D.pdf?OpenElement

Hartman, H.I. (1987). Introductory Mining Engineering. New York: Wiley.

Institute of Electrical and Electronics Engineers (2018). Wireless local area networks (IEEE 802.11). Retrieved from http://www.ieee802.org/11

International Society of Automation (ISA) IEC 62443: Network and system security for industrial-process measurement and control. Retrieved from https://www.isa.org/store/ansi/isa-62443-2-4-2018-/-iec-62443-2-42015amd12017-csv,-security-for-industrial-automation-and-control-systems,-part-2-4-security-program-requirements-for-iacs-service-providers-iec-62443-2-42015amd12017-csv,-idt/62744641

International Organization for Standardization (2017). Information technology – Generic cabling for customer premises – Part 1: General requirements (ISO/IEC 11801-1). Retrieved from https://www.iso.org/standard/66182.html

Lundmark, P. (n.d). Control room ergonomics with the operator in focus for an attractive environment [White paper]. ABB Ltd. Retrieved from https://library.e.abb.com/public/0c863836b06a0818852575ac00620b97/1463_Lundmark_Control_Final.pdf

Mahan, R.E., Burnette, J.R., Fluckiger, J.D., Goranson, C.A., Clements, S.L., Kirkham, H., & Tews, C. (2011). Secure Data Transfer Guidance for Industrial Control and SCADA Systems. US Department of Energy, Pacific Northwest National Laboratory. Report PNNL-20776._Retrieved from https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20776.pdf

Mast, J. (2007). OSU/IME Human Factors Design and Evaluation Checklist; Ohio State University.

Mine Design Technologies (2018): Safety solutions in hard rock mining: wireless geotechnical monitoring; Retrieved from https://mdt.ca/industries/mining/underground-solutions/hard-rock-mining-solutions/

Ministerio de Justicia (2015). Decreto Supremo No. 038-2003-MTC. Retrieved from https://www.osiptel.gob.pe/repositorioaps/data/1/1/1/par/ds038-2003-mtc-limites-radiaciones/ds038-2003-mtc-limites-radiaciones-no-ionizantes.pdf

Ministerio de Transportes y Communicaciones (2018). Website. Retrieved from https://www.gob.pe/mtc

National Telecommunications and Information Administration (NTIA) (2018). Website. Retrieved from https://www.ntia.doc.gov/

National Association of Regulatory Utility Commissioners (NARUC) (2018). Website. Retrieved from https://www.naruc.org/

Peru Ministerio de Transportes y Comunicaciones (2018). La Dirección General de Control y Supervisión de Comunicaciones (DGCSC). Retrieved from http://portal.mtc.gob.pe/comunicaciones/control_supervision/index.html

Sistema Peruano de Información Jurídica (2015a). Decreto Supremo No. 016-2010-MTC. https://gobpe-production.s3.amazonaws.com/uploads/document/file/19219/1_0_1881.pdf

Sistema Peruano de Información Jurídica (2015b). Decreto Supremo No. 013-93-TCC. Retrieved from https://www.osiptel.gob.pe/repositorioaps/data/1/1/1/par/ds013-93-tcc-tuo-ley-de-telecomunicaciones/DS013-93-TCC-TUO-Ley-de-Telecomunicaciones.pdf

Sistema Peruano de Información Jurídica (2015c). Decreto Supremo No.020-2007-MTC. Retrieved from http://transparencia.mtc.gob.pe/idm_docs/normas_legales/1_0_2137.pdf

State of Nevada (2017). Telecommunications—Public Utilities Commission of Nevada (PUCN). Retrieved from http://puc.nv.gov/Utilities/Telecommunications/

State of Colorado (2018). Telecommunications—Colorado Department of Regulatory Agencies (DORA). Retrieved from https://www.colorado.gov/pacific/dora/telecommunications

Wickens, C.D., Lee, J.D., Liu, Y., and Becker, S.E.G. (2004): An Introduction to Human Factors Engineering, 2nd edition, New Jersey: Pearson Prentice Hall.

APPENDIX A: REGULATORY BODIES

Tables A1–A5 are examples of countries with mining activities and relevant regulatory bodies. These jurisdictions were selected to provide regional examples (i.e., Australia, Asia, Africa, and North and South America).

APPENDIX B: TECHNOLOGY SPECIFICS

Table B1 is a list of commonly available networking technologies. A communication system can be composed of the elements presented here but is not limited to them. The technologies presented in each layer (physical, network, transport, and application) might also be used in another layer depending on the conditions and desired output.

Table B1 allows the reader to evaluate the strengths and weaknesses of each potential communications technology.

Because each mine will require a customized networking solution depending on its unique needs, each communication system must also be examined based on its compatible applications (Table B2) and specific characteristics (Table B3).

Table A1. Regulatory Bodies Relevant to Australia

Statutory authority	Description	Citation
Australian Communications and Media Authority (ACMA)	Independent statutory authority tasked with ensuring most elements of Australia's media and communications legislation, related regulations, and numerous derived standards and codes of practice operate effectively and efficiently, and in the public interest. The ACMA is also a "converged" regulator, created to bring together the threads of the evolving communications universe, specifically in the Australian context the convergence of the four "worlds" of telecommunications, broadcasting, radio communications, and the Internet.	ACMA, 2018
Legislative acts		
Australia Telecommunications Act 1997	Section 376 for specified customer equipment and customer cabling	Australian Government, 1997
Australia Radio-communications Act 1992	Section 162 for radio communications, electromagnetic compatibility and electromagnetic energy	Australian Government, 1992
Australia Broadcasting Services Act 1992	Section 9A for digital broadcasting reception equipment	Australian Government, 2018
Western Australia Electricity Act 1945	Licensing of competent people to carry out work relating to electricity and the examination, prohibition or approval of electrical appliances	Government of Western Australia, 2013
Western Australia Electrical Requirements 2015	Minimum requirements for all electrical installations in Western Australia	Government of Western Australia, 2015
Western Australia Mines Safety and Inspection Act 1994	Consolidates and amends the law relating to the safety of mines and mining operations and inspecting and regulating of mines, mining operations and plant, and substances supplied to or used at mines, and promoting and improving the safety and health of people at mines	Government of Western Australia, 2018c
Western Australia Mines Safety and Inspection Regulations 1995	Regulates certificates of competency, procedure for the resolution of disputes, notifications of commencement of suspension of mining operations, inspection of workplaces, safety, electricity, ventilation, and radiation	Government of Western Australia, 2017
Western Australia Occupational Safety and Health Act 1984	Manages the commission for occupational safety and health; workplace duties; safety and health representatives, committees, magistrates, and inspectors; the occupational safety and health tribunal; and legal proceedings	Government of Western Australia, 2018a
Western Australia Occupational Safety and Health Regulations 1996	Regulates workplace safety requirements, plant design, hazardous substances, and performance of high-risk work	Government of Western Australia, 2018b
Standards		
AS/NZS 4240.1:2009	Remote control systems for mining equipment: design, construction, testing, installation, and commissioning	Australian/New Zealand Standard, 2009a
AS/NZS 4240.2:2009	Remote control systems for mining equipment: operation and maintenance for underground metalliferous mining	Australian/New Zealand Standard, 2009b
AS/NZS 2802:2000	Electric cables - Reeling and trailing for mining and general use (other than underground coal mining)	Australian/New Zealand Standard, 2000

Table A1. Continued.

Statutory authority	Description	Citation
AS/NZS 2967:2014	Optical fibre communication cabling systems safety	Australian/New Zealand Standard, 2014
AS/NZS 3085.1:2004 (R2016)	Telecommunications installations - Administration of communications cabling systems - Administration of communications cabling systems basic requirements	Australian/New Zealand Standard, 2004
AS/NZS 3080:2013	Information technology - Generic cabling for customer premises (ISO/IEC 11801-1:2017, MOD)	International Organization for Standardization, 2017
AS/CA S009:2013	Installation requirements for customer cabling (wiring rules)	Communications Alliance Ltd., 2013

Table A2. Regulatory Bodies Relevant to Peru

Statutory authority	Description	Citation
Ministerio de Transportes y Comunicaciones	Institution in charge of legal themes and the development of telecommunications in Peru. Supported by DGCSC and OSIPTEL	Ministerio de Transportes y Comunicaciones, 2018
La Dirección General de Control y Supervisión de Comunicaciones (DGCSC)	The Directorate General for Communications Supervision and Control (DGCSC) is a line agency that is responsible for controlling and supervising the provision of communications services and activities	Peru Ministerio de Transportes y Comunicaciones, 2018
El Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL)	The Supervisory Agency for Private Investment in Telecommunications is a regulatory public body with a mission to promote competition in the telecommunications market, quality of telecommunications services, and the empowerment of the user	El Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL), 2018
Legislative acts		
Decreto Supremo No. 016-2010-MTC	Legislative Act concerning the use of the radio spectrum for broadcasting services	Sistema Peruano de Información Jurídica, 2015a
Decreto Supremo No. 013-93-TCC	Telecommunications law for Peru	Sistema Peruano de Información Jurídica, 2015b
Decreto Supremo No.020-2007-MTC	General regulations regarding the telecommunications law for Peru	Sistema Peruano de Información Jurídica, 2015c
Decreto Supremo No. 038-2003-MTC	Establishes the maximum permissible limits of non-ionizing adiation in telecommunications	Ministerio de Justicia, 2015

Table A3. Regulatory Bodies Relevant to the United States of America

Statutory authority	Description	Citation
Federal Communications Commission (FCC)	Regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia, and US territories. An independent US government agency overseen by Congress, the commission is the United States' primary authority for communications law, regulation, and technological innovation	Federal Communications Commission (FCC), 2018
National Telecommunications and Information Administration (NTIA)	Part of the US Department of Commerce. It is the Executive Branch agency that is principally responsible for advising the President on telecommunications and information policy issues. NTIA's programs and policymaking focus largely on expanding broadband Internet access and adoption in the United States, expanding the use of the radio spectrum by all users, and ensuring that the Internet remains an engine for continued innovation and economic growth	National Telecommunications and Information Administration (NTIA), 2018
National Association of Regulatory Utility Commissioners (NARUC)	NARUC is the national association representing the state public service commissioners who regulate essential utility services in each state. NARUC members are responsible for assuring reliable utility service at fair, just, and reasonable rates	National Association of Regulatory Utility Commissioners (NARUC), 2018
Public Utilities Commission of Nevada (PUCN)	Regulates providers of local telecommunications in Nevada	State of Nevada, 2017
Colorado Department of Regulatory Agencies (DORA)	Commission for telecommunications in Colorado	State of Colorado, 2018

Table A4. Regulatory Bodies Relevant to Ghana

Statutory authority	Description	Citation
National Communications Authority (NCA)	Government body that authorizes all technology equipment and their usage in Ghana It usually assigns frequency usage and communication towers, similar to the US FCC	Ghana National Communications Authority (NCA), 2018
Ghana Civil Aviation Authority (GCAA)	Provides permits and approval for the use of drones, registration and marking of aircraft, and determines requirements for instruments and equipment necessary for flight	Ghana Civil Aviation Authority (GCAA), 2016
Environment Protection Agency (EPA)	Involved in mine permitting, especially if communication towers or other similar technologies are required	Ghana Environment Protection Agency (EPA), 2018
Minerals Commission (MINCOM)	Scope and approval from MINCOM might be needed to obtain a mine permit, depending on the issue at hand	Ghana Ministry of Lands and Natural Resources, 2016

Table A5. Regulatory Bodies Relevant to Mongolia

Statutory authority	Description	Citation
Communications Regulatory Commission of Mongolia (CRC)	Responsible for communications law; similar to the Australian ACMA	Communications Regulatory Commission of Mongolia (CRC), 2018
General Agency for Specialized Investigation (GASI)	Responsible for mining law enforcement; similar to the US Mine Safety and Health Administration (MSHA)	General Agency for Specialized Investigation (GASI), 2016
Legislative acts		
Law of Mongolia on Communications	Laws regulating relations between people creating, using and protecting communication networks in Mongolia	Communications Regulatory Commission of Mongolia, 2001
Law of Mongolia on Radio Wave	Laws regulating the distribution, use, protection, ownership, and possession of radio waves	Communications Regulatory Commission of Mongolia, 1999
Regulation Information and Communication Network of Mongolia	List of regulations for communications in Mongolia	Communications Regulatory Commission of Mongolia, 2013
Directions, terms, and requirements of procedures and regulations	List of procedures for communications in Mongolia	Communications Regulatory Commission of Mongolia, 2016a
Standards		
Mongolian communications standards	List of standards for communications in Mongolia	Communications Regulatory Commission of Mongolia, 2016b

Table B1. Technology Characteristics

Type	Technology	Complexity	Signal attenuation	Typical coverage	Interference/ noise resistance	Maintenance (daily and incidental)	Capacity (bandwidth)
Physical layer (OSI: layer 1)							
Copper (twisted pair)	UTP Cat5/6/7	Low	High	Low	Medium	Low	High
Copper (coaxial)	RG6, RG11, Ava5-50, land mobile radio (LMR), other "non-leak" cable	Low	Medium	Medium	High	Low	High
	Leaky feeder (VHF/UHF)	Low	High	Low	Low	Low	Medium
RF	High frequency/ VHF/UHF/microwave	Medium to high (frequency dependent)	Low	Very high (if not obstacle or curvature)	Low	Medium	High
Optical	Fibre optic	Low	Low	High	High	High	High
Modulation techniques used in physical layer1	Spread spectrum (frequency hopping) radios	Medium	N/A	Medium	High	Low	High
	Modulation (e.g.: OFDM, QAM, PSK, AM, FM)	Medium	N/A	High	Low (AM) to medium (PSK, FM)	Medium	High
Transport layer (Delivers technology) (OSI:layer 4)							
	Ethernet	Low	N/A	Low	High	Low	High
	Wi-Fi (80N2.11)	Low	N/A	Medium	Medium	Medium	High
	WiMAX® (802.16)	Medium	N/A	High	Medium	High	High
	Infiniband	Low	N/A	Very low	Low	Low	Very high
	Token ring / FDDI	Low	N/A	Low	Low	Low	Low
	Fibre Channel	Low	N/A	Low	Low	Low	Very high
	Bluetooth transmitters/ receivers	Low	N/A	Low	Low	Low	Low
	(DOCSIS®)	Medium	N/A	High	High	Medium	High
Network layer (end points)(OSI: layer 3)							
	Digital RF (i.e., DMR, TETRA, P25)	Medium	N/A	Very high	Medium	Medium	Low
	LTE (4G and up)	High	N/A	High	Medium	High	High
	RFID transmitters/ receivers	Low	N/A	Low to medium	Medium	Low	Low
	Spread spectrum	Low	N/A	Medium	Medium	Low	Medium

Table B1. (Continued)

Latency (based on same distance)	Security (data)	Safety (intrinsically safe)	Availability	Reliability	Resiliency	Capable of redundancy	Maturity	Battery-power compatible	Mobility	Cost
Physical layer (OSI: layer 1)										
Low	Medium	Medium	High	High	Medium	Yes	High	Yes	No	Low
Low	Medium	Medium	High	High	Medium	Yes	High	Yes	No	Low
Low	Low	Low	Medium	Medium	Medium	Yes	High	Yes	No	Low
Medium	Low	Low	Medium	Medium	High	Yes	High	Yes	Yes	Medium to high
Low	High	High	High	High	Medium	Yes	High	Yes	No	Medium to high
Low	Medium	N/A	Medium	Low	N/A	N/A	High	Yes	N/A	Low
Low	Low	N/A	Medium	Medium	N/A	N/A	High	Yes	N/A	Medium
Transport layer (Delivers technology) (OSI:layer 4)										
Low	Low	N/A	High	High	N/A	N/A	High	Yes	N/A	Low
Low	Medium to high (if encrypted)	N/A	Medium	Medium	N/A	Yes	High	Yes	Yes	Medium
Low	Medium to high (if encrypted)	N/A	Medium	Medium	N/A	Yes	High	Yes	Yes	High
Very low	High	N/A	High	High	N/A	N/A	High	Yes	N/A	Medium
Low	Medium	N/A	High	High	N/A	N/A	High	Yes	N/A	High (obsolete)
Very low	Medium	N/A	High	High	N/A	N/A	High	Yes	N/A	Low
Low	Medium to high (if encrypted)	N/A	Low	Low	N/A	No	High	Yes	Yes	Low
Low to medium	Low	N/A	Medium	Medium	N/A	N/A	High	Yes	N/A	Low
Network layer (end points)(OSI: layer 3)										
High	Medium to high (if encrypted)	N/A	High	High	N/A	Yes	High	Yes	Yes	Medium
Medium	Medium to high (if encrypted)	N/A	Medium	High	N/A	Yes	Medium	Yes	Yes	High
Low	Medium to high (if encrypted)	N/A	High	High	N/A	No	Medium to high	Yes	Yes	Low
Low	Medium to high (if encrypted)	N/A	Medium	Medium	N/A	No	High	Yes	Yes	Low

Table B1. (Continued)

Type	Technology	Complexity	Signal attenuation	Typical coverage	Interference/ noise resistance	Maintenance (daily and incidental)	Capacity (bandwidth)
Network layer (end points)(OSI: layer 3) (continued)							
	HSPA (3G)	Medium	N/A	High	Medium	Medium	Medium
	Telephone/mobile phone	Medium to high	N/A	N/A	Medium	High	N/A
Application layer (End points) (OSI: layer 7)							
	Pagers	Low	N/A	N/A	Medium	Low	N/A
	2-way radio	Low	N/A	N/A	Low to medium	Low	N/A
	Bluetooth devices	Low	N/A	N/A	Low	Low	N/A
	RFID tag	Low	N/A	N/A	Low	Low	N/A

Table B1. (Continued)

Latency (based on same distance)	Security (data)	Safety (intrinsically safe)	Availability	Reliability	Resiliency	Capable of redundancy	Maturity	Battery-power compatible	Mobility	Cost
Physical layer (OSI: layer 1)										
Medium	Medium to high (if encrypted)	N/A	Medium	High	N/A	Yes	High	Yes	Yes	Medium
N/A	Medium	Medium	High	Medium	Low	No	High	Yes	Yes	Low to medium
Application layer (End points) (OSI: layer 7)										
N/A	Low	Medium	High	High	Medium	No	High	Yes	Yes	Low to medium
N/A	Medium to high (if encrypted)	High (if using specific model)	High	High	High	No	High	Yes	Yes	Low to medium
N/A	Low	High	High	Low	Low	No	Medium to high	Yes	Yes	Low
N/A	Low	High	High	High	Very high	No	Medium to high	Yes	Yes	Very low

Table B2. Characteristics of Specific Communications Systems

Infrastructure Technology	Wired			Optical
	Telephone	Paging	LAN	LAN
Media	Copper cabling	Mixed	CAT5e CAT6 coaxial	Fiber optic
Characteristics				
Infrastructure investment	Low	Low	Low	High
Infrastructure complexity	Simple interference possible	Simple	Moderate	Moderate-high
Interference proof	Electrical	RF	Electrical interference possible	Yes
Maintenance	Low 90 m over copper	Low	Moderate	Moderate-high
Signal attenuation	Limited to (10/100/10 Mbits)	Yes	Limited to 90 m over copper	Depends on wavelength
Capacity	Ethernet	Unknown	Ethernet (1G / 10G) or lower	1G / 10G / 40G using Ethernet
Latency	Low	Unknown	Low	Low
Data security	Encryption	Unknown	Encryption	Encryption (optical layer more difficult to decode)
Safety (detonator friendly)	Yes	–	Yes	Yes
Availability	Good	Unknown	Very good	Very good
Reliability	Good	Unknown	Very good	Very good
Resiliency	Good	Unknown	Good (if using proper armored cable)	Good (if using proper armored cable)
Capable of redundancy	Limited[1]	Unknown	Yes	Yes
Maturity	High	High	High	High
Battery-power compatible	Yes	Yes	Yes	Yes
Mobility	Yes (wi-fi)	Yes	Yes	No

1. The infrastructure can be redundant but the telephone is a single point of failure; 2. 802.11ac supports approx 1.3 Gbit of data up and down; 3. Around 170 Mbit down and 60 Mbit up for a typical 20 MHz 2x2 setup. May increased if RF bandwidth is increased (i.e.: more channels).

	Radio					Hybrid		
2-way radios	**Ultrawide Band (UWB)**	**Wi-Fi**	**Wi-Fi**	**Cellular Network (LTE)**	**Leaky feeder VHF/UHF**	**DOCSIS 3 (coaxial)**	**RFID**
Radio waves	Radio waves	Radio waves	Radiating cable	Radio waves	Radiating cable	Coaxial cables	Radio waves
Low	Low-moderate	High	High	High	Moderate	Moderate	Low-moderate
Simple	Simple	Moderate-high (controller-based)	Low	Moderate-high	Low	Low	Low-Low-moderate
No	No	No	No	No	No	No	No
Low	Low	Low-moderate	Moderate	Moderate	Low	Low	Low
Depends on frequency	Low	Depends on frequency	Depends on frequency	Depends on frequency	Depends on frequency	Moderate	High
< 1 Mbits	< 1 Mbits	Depends on RF bandwidth and RF Stream[2]	Depends on RF bandwidth and RF Stream[2]	Depends on RF bandwidth and RF Stream[2]	Few Mbits at most	10G or less	N/A
High	High	Low	Low	Low	Medium-high	Low	Medium-high
Encryption	Encryption	Encryption	Encryption	Encryption	Encryption	Encryption	Limited
Potential risk	Potential risk	Potential risk	Potential risk	Potential risk	Potential risk	Yes	Yes
Good	Good	Good	Good	Good	Very good	Very good	Good
Good	Good	Good	Good	Good	Very good (if properly maintained)	Very good	Medium
Rugged	Rugged	Good (if using proper rugged equipment)	Good (if using proper rugged equipment)	Good (if using proper rugged equipment)	Good (if using proper armored cable)	Good (if using proper armored cable)	Good (if using proper armored cable)
Yes	Yes	Yes (if using multiple frequency and access points)	Yes (if using multiple frequency and access points)	Yes (if using multiple RRUs)	Yes (using digital radio system with 2 carriers)	Yes if using multiple CMTS	No
High	Medium	High	High	High	High	High	Medium-high
Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table B3. Applications of Specific Communications Systems

Infrastructure Technology	Wired			Optical
	Telephone	Paging	LAN	LAN
Application				
VoNice	Yes	Yes	Yes	Yes
Video	Yes (IP phone)	No	Yes	Yes
Micro date	Yes (SIP devices)	No	Yes	Yes
Ventilation on demand (VOD)	No	No	No[2]	No[2]
Continuous tracking	No	No	No[2]	No[2]
Automated mobile equipment	No	No	No	No
Automated stationary equipment	No	No	Yes	Yes
Fleet monitoring	No	No	Yes	Yes
RFID (proximity)	No	No	No	No
Real-time data monitoring	No	No	Yes	Yes
Tele-operated equipment	No	No	Yes	Yes
Environmental monitoring (gas/air/seismic)	No	No	Yes	Yes
Continuous mining	No	No	No	No
Fire detection	No	No	No	No
Personnel tracking	No	No	No	No
Blasting	No	No	Yes	Yes
Collision avoidance	No	No	No	No

1. Wired and optical have the same applications. The only difference is the distance achievable. Optic offers better distance, and wired offer "power-over-wire" which is useful to power up sensors. Both can do 100m, 1Gbit, 10gbit; 2. Needs tracking device in conjunction with root system for mobile applications; 3. Applicable for stationary equipment; 4. Input-output on digital radio can control/monitor data; 5. Low bandwidth on digital radio can provide monitoring function.

Radio					Hybrid		
2-way radio	Proprietary wireless technology (e.g., frequency hopping, different OFDM technologies, nanotron)	Through-the-Earth (TTE)	Wi-Fi network (LTE)	Cellular	Leaky feeder VHF/UHF	DOCSIS 3 (coaxial)	RFID
Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
No	Yes	No	Yes	Yes	Yes	Yes	No
Yes[4]	Yes	No	Yes	Yes	Yes	Yes	No
No	Yes	No	Yes	Yes	Yes	Yes	No
No	Yes	No	Limited	No	Yes	Yes	No
No	N/A	No	Yes	Yes	No	Limited	No
No	N/A	No	Yes	Yes	No	Yes	No
No	Yes	No	Yes	Yes	Limited	Limited	No
Yes	N/A	No	Limited	No	No	Yes	Yes
Yes[5]	Yes	No	Yes	Yes	Yes	Limited	No
No	N/A	No	Yes	Yes	No	Yes	No
Yes[5]	Yes	No	Yes	Yes	Yes	Yes	No
No	N/A	No	Yes	Yes	No	No	No
No	No	No	No	No	No	No	No
Yes	Yes	No	Yes	Yes	No	No	Yes
Yes	Yes	No	Yes	N/A	Yes	Yes	No
No	Yes	No	Yes	Yes	No	No	Yes