SME Annual Meeting
Feb. 23 - 26, 2014, Salt Lake City, UT

Preprint 14-026

UNDERGROUND COAL MINE TRACKING AND COMMUNICATION SYSTEM RELIABILITY AND AVAILABILITY METHODOLOGY

R. Wisniewski, Reliability Information Analysis Center, Utica, NY
S. Schafrik, Virginia Tech, Blacksburg, VA

ABSTRACT

Every underground coal mine in the United States must deploy and operate a wireless communication and tracking system. This paper addresses the reliability and availability of an installed tracking system and the communications infrastructure that supports it. A particular interest is the requirements for the systems to operate continuously without failure after a mine disaster for 96 hours, and the requirements in the MINER Act for the tracking systems to be "calculated to be serviceable" and the communications systems "redundancy". These requirements imply a certain reliability and availability. This paper describes a quantitative way to assess these systems requirements, using the tools that are available and commonly used by the Reliability, Maintainability, & Availability community.

INTRODUCTION

On its most basic level, **reliability** can be defined as the probability that an item (or system) will perform its intended function for a specified interval under stated conditions (Nicholls 2005). If a system is performing its intended function for a specified interval under stated conditions, it is said to have **mission success** or **success**. Hence, the terms reliability and **probability of success** are often used interchangeably. A statement of reliability has four key components:

1. *Probability* – For example, a radio might have a reliability goal of 0.9995. This would mean that at least 99.95% (or 9,995 out of 10,000 units) would still be functioning at the end of the stated time period. Stated another way, a radio would have a 99.95% chance of being operational at the end of the stated time period.

2. *Intended function* – This should be defined for every part, subassembly, assembly, component and system. The statement of the intended function should state or imply a failure definition. For example, suppose a fan's intended function is to move at least 3000 CFM of air. The implied failure definition would be moving less than 3000 CFM of air.

3. *Stated conditions* – These include environmental, maintenance, usage, storage and moving and possible additional conditions.

4. *Specified period of time* – This is the time interval over which the system is expected to function and meet the reliability requirement. This interval can begin when the system is installed and ready for operation. For example, a radio may be required to have a reliability of 95% over a period of 5 years. This would mean that a radio would have a 95% probability of still being operational at a time of 5 years following first use. Alternatively, a specified period of time may begin upon the occurrence of a specific event. For example, a mine tracking system might be required to have a reliability of 95% for a period of 96 hours following a catastrophic event such as a roof collapse. This would mean that the system would have a 95% probability of still being operational at a time of 96 hours following the event. It should be noted that the reliability functions discussed in the following sections assume that a system is fully operational at time = 0, where t = 0 is the time of event occurrence. If system testing/diagnostics are such that it cannot be determined that the system is fully operational at the occurrence of an event, then one would have to look back to the previous point in time when this could be established and add this time to the specified operational time for the purposes of calculating reliability. The required operating time plus the time of the last successful determination of system operation to the event occurrence is referred to as the **exposure time.** If in the above example, the system undergoes a complete diagnostic test and inspection once every week, then the total exposure time that should be used for calculating reliability is 96 hours operating time plus 168 hours latent time for a total of 264 hours.

The **reliability function** for an item quantifies the probability that it will perform its intended function for a specified interval under stated conditions (Nicholls 2005). In the case of systems and software, the exponential distribution is the most commonly used model for determining item reliability. The reliability function using the exponential distribution is given by the following:

$$R(t) = e^{-\lambda t} \text{ or } R(t) = e^{-\frac{t}{MTBF}}$$

Where,

R(t) = Probability of successful performance over time period "t" (i.e., "reliability")
t = Time period of interest (in units consistent with λ or MTBF) (may need to include exposure time)
λ = Measured, predicted or estimated **failure rate** of the item
MTBF = 1/λ = Measured, predicted or estimated **mean time between failure** of the item

The **unreliability**, or **probability of failure** (Nicholls 2005), of an item is given by:

$$F(t) = 1 - R(t)$$

The **failure rate function** defines the rate per unit time that a failure will occur over a defined time period (e.g., calendar hour, operating hour, CPU execution hour, etc.) It can be calculated by dividing the number of inherent failures experienced by the total time period over which those inherent failures were experienced (Nicholls 2005). For example, if an item experiences 5 failures over 20,000 operating hours its failure rate can be calculated as:

$$\lambda = \frac{5\ failures}{20000\ operating\ hours} = 0.00025\ failures\ per\ operating\ hour$$

The **Mean Time Between Failure (MTBF)** represents the average expected time from the occurrence of one failure to the occurrence of the next failure (Nicholls 2005). MTBF is traditionally applied to repairable systems, and includes only inherent failures within a system. Actions resulting from scheduled preventive maintenance, or from induced and can-not-duplicate (CND) incidents are not counted toward MTBF (but would be counted if the measure is Mean Time Between Maintenance – MTBM). MTBF can be calculated from the reciprocal of the failure rate (1/λ). For example, if an item

failure rate is 0.00025 failures per hour, then the MTBF can be calculated as 1/0.00025, or 4,000 hours.

If only failures that are critical to system performance or mission success are assessed, then the resulting calculation will be **Mean Time Between Critical Failure (MTBCF)**. This means that failures may occur in use, but if they do not result in the loss or excessive degradation in a critical system function, then they are not counted in the MTBCF calculation. **Mean Time To Failure (MTTF)** is analogous to MTBF and is applied to non-repairable systems (Nicholls 2005).

AVAILABILITY

Availability is a measure of the likelihood that a system will be ready to operate when it is called upon to operate. Reasons for the system not being ready to operate include (1) the possibility that a failure has occurred and the repair has not been completed and (2) the possibility that the system is not operable because preventive maintenance actions are necessary. Therefore, it can be said that availability is a function of the failure rate of the system, the number and type of maintenance actions necessary, and the time it takes to complete those actions.

In general, there are two types of maintenance actions – preventive and corrective. **Preventive maintenance** includes all actions taken to keep a system operational by preventing wearout failures. Preventive maintenance does not reduce the constant failure rate of a system, but tends to maintain its inherent level of failure probability. If preventive maintenance actions can be planned and executed when there is no demand to use the system, then availability will not be affected. **Corrective maintenance** includes all actions that are required to return the system to an operating state once a failure has occurred. Corrective maintenance cannot be planned and must be performed when the system fails. The mean time that is required to bring a system back to an operational state after a failure has occurred is referred to as the **mean time to repair (MTTR)**. MTTR includes only that time associated with the identification, isolation, repair/fix and verification of repair/fix activities for actual failures (Nicholls 2005). Logistical and Administrative delay times and normal scheduled preventive maintenance times are not included in the calculation of MTTR.

There are several different measures of availability, including inherent availability, achieved availability, operational availability and uptime ratio.

Inherent Availability is dependent upon the MTBF and the MTTR, where MTTR refers to corrective maintenance only. Inherent availability excludes downtime due to preventive maintenance and logistics/administrative delays. In other words, it reflects the percentage of time that a system would be available if no delays were experienced due to maintenance, supply of replacement parts, supply of qualified repair personnel, etc., (i.e., not design related). The expression for inherent availability is given as:

$$A_{\text{h}} = \frac{MTBF}{MTBF + MTTR} \times 100\%$$

Achieved Availability is dependent upon the mean time between maintenance (MTBM) and the active mean time to repair ($MTTR_{Active}$), where MTBM includes preventive and corrective maintenance activities, and $MTTR_{Active}$ is the mean time to accomplish preventive and corrective maintenance tasks. Achieved availability is similar to inherent availability, except that preventive and corrective maintenance are included in the parameter. However, logistics/administrative delay times are not considered for achieved availability. The expression for achieved availability is given as:

$$A_{\cdot} = \frac{MTBM}{MTBM + MTTR_{\text{@sh}}} \times 100\%$$

Operational Availability is similar to achieved availability, except that it includes logistics and administrative delays. Operational availability is dependent upon MTBM (preventive and corrective) and the mean down time (MDT), which includes $MTTR_{Active}$ and all other downtime such as maintenance delays and other non-design factors. Operational availability reflects the totality of the inherent design of the system, the availability of maintenance personnel and spares, maintenance policy and concepts, and other non-design factors. The expression for operational availability is given as:

$$A_{\text{n}} = \frac{MTBM}{MTBM + MDT} \times 100\%$$

Uptime Ratio is dependent upon the total time that the system is in the customer's possession and works and the total time that the system is not operable/usable. The expression for uptime ratio is given as:

$$A = \frac{Uptime}{Uptime + Downtime} \times 100\%$$

Uptime ratio is time dependent; the time period over which the measurement is made must be known. For example, if a failure occurs in the first 25 hours of operation and requires one hour to correct, the uptime ratio is 24/(24+1) = 96% availability. If operation then continues failure free for another 25 hours, the availability for the first 50 hours is 49/(49+1) = 98%. Uptime ratio is typically calculated from experience data as operational time and downtime is accumulated.

A given level of availability can be achieved with different combinations of values of reliability and maintainability. As reliability decreases, better maintainability is needed to achieve the same availability. Likewise, as maintainability decreases, better reliability is required if availability is not to be impacted.

RELIABILITY MODELING

A system can be modeled for reliability analysis through the use of block diagrams. A system consists of subsystems connected to perform various functions. Systems can become complex, making reliability analysis difficult. A math model that reduces a system to a graphical representation of the interconnection of its subsystems can be used to present a clear picture of the functional interdependencies and provide a framework for developing quantitative system level estimates to guide the design trade-off process. Models are helpful for the following:

- Easy identification of single points of failure
- Making numerical allocations
- Evaluating complex redundant configurations
- Showing all series-parallel relationships
- Allowing summarization of all factors affecting system reliability

Models are derived from, and traceable to, functional requirements. They may take inputs from reliability predictions, test data, field data, customer requirements and use profiles. Models may range from being relatively simple to quite complex while considering details such as duty cycles, service life limitations, wearout items, varying environments, dormant conditions, human reliability and software. The scope of the model usually depends upon the type and amount of information available for use and the criticality of the system under consideration.

Series Model

The most basic form of a reliability block diagram is the **series model**. A reliability series model block diagram indicates that successful system functioning depends upon all subsystems being operational. Failure of any one of the subsystems causes the system to fail. Many, if not most, systems are designed in this manner unless some effort is made to incorporate redundancy into the design.

An example of a series reliability block diagram containing three subsystems is shown in Figure 1.

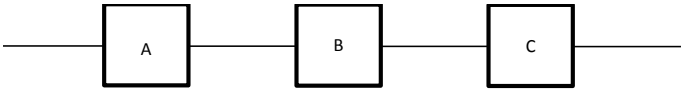

Figure 1. Series Model Containing Three Subsystems.

The reliability of a system, R(t), is the probability of success of the system for mission time "t". For a system composed of subsystems in a series model, the system reliability is the product of the subsystem reliabilities. The reliability of a subsystem, $R_i(t)$, is the probability of success of that subsystem over mission time "t". In general, for a system composed of a series of *n* subsystems, the system reliability can be found from:

$$R(t) = R_0(t) \cdot R_1(t) \cdot R_2(t) \cdot \ldots \cdot R_n(t)$$

For example, in the system depicted in Figure 1 the system reliability would be given by:

$$R(t) = R_C(t) \cdot R_A(t) \cdot R_B(t)$$

Since the reliability for each subsystem will be less than one, it is clear that the system reliability will be less than the reliability of any individual subsystem, and indeed will be less than the reliability of the least reliable subsystem.

While it should be noted that the above equations for system reliability are independent of the choice of distribution used to calculate the subsystem reliabilities, as stated earlier the exponential distribution is often used for modeling item reliability. If the exponential distribution is applied to each of the subsystems, then the reliability of the *i*th subsystem is given by:

$$R_i(t) = e^{-\lambda_i t} = e^{-t/MTBF_i}$$

where λ_i and $MTBF_i$ are the failure rate and MTBF of the *i*th subsystem, respectively.

Parallel Model

Redundancy can be designed into a system to increase system reliability (Nicholls 2005). A system containing redundancy has more than one **parallel** path that provides for system success. A system with **active redundancy** is comprised of subsystems in parallel that are on-line and operating. If a subsystem fails, system success can still be accomplished with the successful operation of one or more of the remaining subsystems. An example of a system containing two active, on-line subsystems such that successful operation of one of them is required for system success is shown in Figure 2.

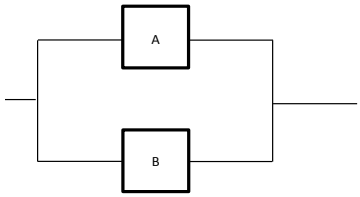

Figure 2. Parallel Model for Two Redundant Systems.

In order to calculate the reliability for a parallel system, it is necessary to assume that the probabilities of failure of each of the subsystems are completely independent over the entire mission time. In order to ensure the validity of this assumption it is necessary that the system be designed in such a manner that the failure of one subsystem does not affect the reliability of the remaining subsystems, and that a single event does not cause more than one subsystem to fail (otherwise known as a **single point failure**). If either of these two situations were to occur, then redundancy would be reduced and the improvement in system reliability due to redundancy would be lost. Systems must be carefully analyzed to detect and remove the presence of single point failures if system reliability is to be maximized. Particular attention should be given to power supplies and interconnection points of redundant systems, since these are often the source of single point failures. Sometimes the physical proximity of redundant subsystems to each other must be considered when trying to determine the presence of single point failures. For example, if redundant power supplies for an air circulation system for a mine shaft are located in close enough proximity such that a roof collapse would likely destroy all of them, then this could be a source of a single point failure.

In general, for a system composed in parallel of *n* subsystems such that the reliability of the subsystems is independent and successful operation of one of the subsystems is required for system success, the system reliability can be calculated as "1minus the product of the probability of failure (unreliability) of each subsystem in the redundant configuration" as shown below:

$$R(t) = 1 - [(1 - R_0(t)) \cdot (1 - R_1(t)) \cdot (1 - R_2(t)) \cdot \ldots \cdot (1 - R_n(t))]$$

For example, in the system depicted in Figure 2 the system reliability would be given by:

$$R(t) = 1 - [(1 - R_C(t)) \cdot (1 - R_A(t))]$$

From the above equations, it is clear that the system reliability will be greater than the reliability of any of the redundant subsystems. While it should be noted that the above equations for system reliability are independent of the choice of distribution used to calculate the subsystem reliabilities, as stated earlier the exponential distribution is often used for modeling item reliability. If the exponential distribution is used to model subsystem reliability for the system shown in Figure 2, the system reliability would be given by:

$$R(t) = e^{-\lambda_C t} + e^{-\lambda_A t} - e^{-(\lambda_C + \lambda_A)t}$$

If subsystems A and B are identical, then $\lambda_A = \lambda_B$, and the expression for reliability for the system shown in Figure 2 becomes:

$$R(t) = 2e^{-\lambda_C t} - e^{-2\lambda_C t}$$

Similar expressions for system reliability can be derived for 1 out of 3, 1 out of 4, through 1 out of *n* redundant subsystems.

***m*-out-of-*n* System Model**

A special case of the parallel system is the *m*-out-of-*n* system. This type of system is comprised of *n* equivalent subsystems of which a total of *m* must be operating in order to achieve system success. For this system, *m* may be any integer less than *n*. If *m* = 1, then the system reduces to an active parallel system. If *m* = *n*, then the system reduces to a series model.

The expression for the reliability of an *m*-out-of-*n* parallel system in which all units are active, independent and identical is given by:

$$R(t) = \sum_{k=m}^{n} \frac{n!}{k!\,(n-k)!} (R)^k (1-R)^{(n-k)}$$

where R is the reliability of one of the redundant subsystems at time "t".

If the exponential distribution is used to model subsystem reliability, the system reliability would be given by:

$$R(t) = \sum_{k=m}^{n} \frac{n!}{k!\,(n-k)!} \left(e^{-\lambda t}\right)^k \left(1 - e^{-\lambda t}\right)^{(n-k)}$$

Standy Redundant Systems

A system that contains parallel units that are utilized only in the event of a failure is a **standby redundant system** (Nicholls 2005). Such a system typically contains a sensor that can detect a failure in the primary unit and a switch that changes the system function from the primary to the standby unit. The standby unit must be capable of performing the function, but it might not be identical to the primary unit. The sensing and switching system may be an automatic part of the system or it may require a manual interface. An example of a standby redundant system would be a mine elevator that is powered by one of three sources. The primary source would be line voltage from a power utility. The standby power sources would be a diesel generator and a battery backup system. If a drop in line voltage from the utility is detected, a diesel generator would be started to maintain power. If the diesel generator were to fail, power supplied from a bank of batteries would be used to operate the elevator.

Series-Parallel Model

As systems become more complex, it may be necessary to model them as a combination of series and parallel subsystems. In this case,

the same assumptions apply as for individual series or parallel systems. The combined system reliability can be calculated by converting the system into an equivalent series or parallel system and using the appropriate reliability equations.

RELIABILITY MODELING PROCESS

As stated earlier, a system can be modeled for reliability analysis through the use of block diagrams. A system consists of subsystems connected to perform various functions. Systems can become complex, making reliability analysis difficult. A math model that reduces a system to a graphical representation of the interconnection of its subsystems can be used to present a clear picture of the functional interdependencies and provide a framework for developing quantitative system level estimates to guide the design trade-off process. An overall process flow diagram for the construction of Figure 3.

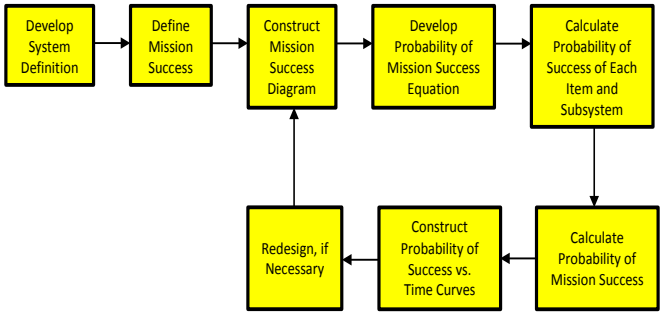

Figure 1. Reliability Modeling Process Flow.

The process of constructing a reliability model begins with a clear definition of the system as related to the definition of reliability. The system reliability model and mission success definition can become elusive problems, especially for multimodal systems incorporating redundancies and alternate modes of operation. In system definition, emphasis is placed on properly specifying reliability within the context of all other pressing requirements and constraints that comprise a functioning system. Since system reliability is defined as the probability of performing a specified function or mission under specified conditions for a specified time, a reliability requirement for mission success must include:

- A definition of item performance such that every condition is defined as acceptable (success) or unacceptable (failure). Clearly, item modes of operation must be known in order to define success or failure.
- A definition of the conditions. This involves defining the environmental conditions which prevail on the various equipment throughout the mission. Additionally, duty cycle or periods of operation must be defined.
- A definition of mission time. A careful quantitative statement of the time during which the system must function is important. If different functional modes or mission stages require the use of certain subsystems, the functioning time requirements for each of the subordinate groups must be established. It should be noted that exposure time might be greater than mission time for a subsystem, depending upon the frequency of periodic maintenance and tests of the system operating status.
- A definition of the reliability variable of the item elements. The reliability variable is a number (time, cycles, events, etc.) used to describe the duration required by each item element.

A complete definition of a system includes the use, performance, restraints and failure definitions. The following steps can aid in the development of this definition.

1. **Define the purpose and intended use or mission of the system.**
   a. Define mission functions and modes of operation.
   b. Define the intended use or mission in terms of performing functions including:
      i. Functional mode of operation – some systems perform multiple functions with different equipment or groups of equipment being required for each function.
      ii. Alternative modes of operation – an item that has more than one method of performing a particular function is said to have alternative modes of operation.

Before a model can be developed, requirements must be formulated and understood. A word statement of reliability (mission success) requirements must be developed and used, along with knowledge of the series-parallel relationships of the various subsystems, to construct a reliability block diagram, which is a pictorial representation of what is required for successful system operation.

2. **Establish and specify the system and subsystem performance parameters and allowable limits.** The list of parameters should be all inclusive, completely defining the entire item under consideration. The allowable limits on these parameters should also be stated.
3. **Determine the physical and functional boundaries of the system.** Physical boundaries include maximum dimensions, weight, safety provisions, human factors restraints, materials capabilities, etc. Functional boundaries must be considered whenever an item is contained in or depends upon another item. In this case, item interfaces (e.g., man-machine interfaces, interface with central control, power sources, data requirements, etc.) must be coordinated for compatibility.
4. **Determine the conditions which constitute mission failure.** Since a failure is an inability to complete a stated mission within specific limits, the conditions that would constitute a mission failure should be identified and listed. For example, it is required that a miner location tracking system not have a blackout area greater than 2000 square feet. In this case, any hardware or software failure or combination thereof that would result in such a blackout area would result in mission failure.
5. **Define the service use profile.** The service use profile is a thorough description of all events and environments associated with an item. The profile depicts expected time spans, environments, operating modes (including standby and ready modes), etc., for each event. The service use profile typically consists of the mission profile and the environmental profile.
   a. **Mission profile** – describes the events and conditions associated with a specific operational usage of a system. Multiple mission profiles may be required to adequately describe a system's multi-mission capabilities. The mission profile must address the system duty cycles and periods of operation. The system should be subdivided into components or subsystems, and a plot of the intended use through time for each should be developed.
   b. **Environmental profile –** describes the specific natural and induced environments (nominal and worst case) associated with operations, events and functions described by the operational cycle. It should be noted that systems, subsystems and components may be utilized in more than one environment. Additionally, a given mission may consist of several phases of operation or periods of time during which a specific environment prevails. For example, sensors used in a miner location tracking system might be required to operate for three months without being cleaned and serviced during normal operating conditions, and for 96

hours without servicing in a coal dust saturated environment following an accident.

Once the system definition has been developed, a reliability model can be constructed using the following steps.

1. Define what is required for mission success and translate this into a mission success diagram.
2. Write the probability of success, R, equation for the system.
3. Calculate the probability of success, R, for each item (component or subsystem) comprising the system. This is done by utilizing field performance data (number of failures vs. operating time), supplier (vendor) test data, data obtained for similar systems that have been previously fielded, or by one of many reliability prediction techniques, including MIL-HDBK-217, 217Plus™, and the Nonelectronic Parts Reliability Data (NPRD) publication (available from http://theriac.org).
4. Insert the probability of success numbers derived for the various components and subsystems in (3) into the system probability of success equation derived in (2).
5. Probability of success curves vs. time can be plotted by taking several values of time for mission time, and evaluating the probability of system success using (2), (3) and (4) for the values of time chosen.
6. Additional steps in the analysis will depend upon the decisions that the analysis is intended to optimize. Such additional steps may include the addition or removal of redundancy, selection of more reliable components, adjusting system test, inspection and preventive maintenance intervals, etc.

RELIABILITY MODELING EXAMPLE – MESH SYSTEM

In this section a meshing communication and tracking system will be used for selected reliability calculations. The meshing system consists of directional antennas wired to node devices by antenna cables and combinations of splitters and connectors external to the node itself. Nodes do share power supplies but not batteries. Functionality overlaps, such as radio cross connections are enumerated only where germane to the example. Each assembly will contain a mixture of items in Table 1 and details of the assemblies is not provided. Table is provided as an example, and should only be used for this particular system in this particular mine. Because of space constraints block diagrams of the complete system are not included in this paper. Table 1 contains the failure rate and abbreviations for each component that will be used. Failure rates are provided in terms of failures per million operating hours and were obtained from NPRD-2011, published by the Reliability Information Analysis Center (RIAC). The failure rates were chosen based upon a high level description of the component. No attempt was made to refer to component vendor data sheets or other literature or performance data in order to determine the validity of these failure rates. Such an analysis is beyond the scope of this report. As a result, the failure rates (and resulting reliability calculations) are provided for illustrative purposes only. The component reliability provided in Table 1 is based upon the failure rate and an exposure time of 96 hours.

Table 1. Component Nomenclature, Failure Rate and Reliability.

Item	Failure Rate (fpmh)	Reliability (at 96 hours)
Power Supply (PSU)	13.234760	0.998730
Battery (BATT)	1.334989	0.999872
Power Supply and Battery (POWER)	N/A	1.000000
Node	23.362303	0.997760
RF Cable (RFft.)	0.594842	0.999943
3 Way Splitter (3WAY)	0.547250	0.999947
YAGI Antenna	19.119576	0.998166

A sample calculation for the power supply unit (PSU) is provided below. Note that the PSU failure rate in Table 1 was converted to failures per hour for use in the reliability equation.

$$R(t) = e^{-\lambda t} = e^{-(0.00001323476)(96)} = 0.998730$$

Each node has a redundant source of power. The primary source is a power supply plugged into line power. A battery backup can supply power for a minimum of 96 hours in the event that line power is interrupted or the power supply fails. Therefore, the power source (POWER) for each node can be modeled as a 1-out-of-2 parallel system. Since the battery will operate only in the event of a PSU failure, the POWER redundancy is determined to be active-standby. However, in order to simplify the calculations for illustrative purposes, POWER will be treated as having active-active redundancy. The model for POWER is shown in Figure 4.

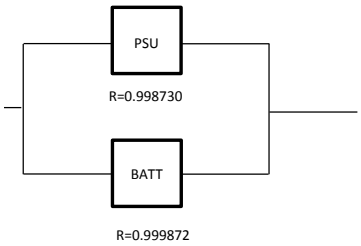

Figure 2. Block Diagram for the Node Power Source (POWER).

The reliability calculation for POWER is given below:

$$R_{\text{ONV DQ}}(t) = 1 - \left(\left(1 - R_{\text{ORT}}(t)\right) \cdot \left(1 - R_{\text{A@SS'S}}()\right)\right)$$
$$R_{\text{ONV DQ}}(t) = 1 - \left((1 - 0.998730) \cdot (1 - 0.999872)\right)$$
$$R_{\text{ONV DQ}}(t) = 1 - (0.00127 \cdot 0.000128)$$
$$= 1 - 0.000000016$$
$$= 0.999999984 = 1.000000$$

Since each node contains a redundant power source, in order to simplify the resulting reliability models the power source will be labeled as “POWER” which will be as defined in Figure 4. This is an example that shows calculations and the simplification that can be achieved with blocks diagrams. Because space constraints, block diagrams will not be presented for the following examples, but it is necessary for analysis of complex systems.

System Model 1: Complete System Operability

According to the system description, a node can communicate with another node in a wireless fashion only if their antennae are within range of each other (direction and proximity). For most fixed mesh nodes this would be the node immediately upstream and downstream. In most instances, a failed node “breaks” the chain of communication and contact with areas deeper in the mine would be lost. Several fixed mesh nodes are set up as crosslinks. That is, they have an antenna positioned so that they can communicate with a node on the adjacent network. In this system, the crosslinks are FMN-202/FMN-102, FMN-204/FMN-105 and FMN-205/FMN-106. If both ends of a crosslink are functional, then it is possible for a signal to bypass a failed node (depending upon the location of the failure). Note, however, that coverage would still be lost at least within the immediate vicinity of the failed node.

Based upon the example system design, with the exception of the gateway nodes, there is no overlapping coverage between nodes. A failure of any portion of a fixed mesh node results in a loss of coverage in a particular area meeting the definition of system failure. Therefore, a series model can be used to describe the system level reliability. The reliability calculation for the system is given below:

$$R_{\text{Rxr sdll}} = R_{\text{F@SD}} \cdot R_{\text{EL M,0/ 0}} \cdot R_{\text{EL M,0/ 1}} \cdots \cdot R_{\text{EL M,1/ 6}} \cdot R_{\text{EL M,1/ 7}}$$

Using the reliability values calculated for each individual node assembly, in a manner similar to the POWER calculation above, the system reliability is:

$$R_{\text{Rxr sdll}} = 0.885840$$

System Model 2: FMN-109 Area Coverage

This example illustrates a calculation for the reliability of providing communication coverage in the proximity of FMN-109.

Note, in order to simplify the discussion that follows, subsystems FMN-XXX will be assumed to be either completely operational ("good") or completely failed ("bad"). This analysis will not consider the effects of failures at the component level, nor will it consider individual failure modes.

According to the system description, the nodes communicate with each other in a daisy chain series fashion, except for:

- FMN-106 which can communicate with FMN-205 and FMN-105
- FMN-204 which can communicate with FMN-203 and FMN-105
- FMN-105 which can communicate with FMN-204 and FMN-104
- FMN-202 which can communicate with FMN-201 and FMN-102
- FMN-102 which can communicate with FMN-202 and FMN-101

One of the initial branches (FMN-105, FMN-104, FMN-103, FMN-102, etc.) is entirely contained in one of the paths from FMN-205, FMN-204. Since any failure or failures along this chain will break both paths, the path proceeding from FMN-205, FMN-204 can be removed from the diagram without any loss of information. Furthermore, the initial chain at the beginning of the diagram (FMN-109, FMN-108, FMN-107, FMN-106) is a simple series model and can be replaced with a single block. The reliability of this combined block is given by:

$$\begin{aligned} R_{@} &= R_{\text{EL M,0/8}} \cdot R_{\text{EL M,0/7}} \cdot R_{\text{EL M,0/6}} \cdot R_{\text{EL M,0/5}} \\ &= (0.993824)(0.993881)(0.993881)(0.993881) \\ R_{@} &= 0.975692 \end{aligned}$$

This same simplification technique for the entire system must be performed. It is clear that the system reliability model is of the complex or non- series/parallel type. Therefore, in order to derive the system reliability mathematical model, repeated use of the following equation must be used

$$R_{\text{RXR}} = R_{\text{RXR+WF nnc}} \cdot R_{\text{W}} + R_{\text{RXR+WA` c}}(1 - R_{\text{W}})$$

where $R_{SYS,X\ Good}$ is the system reliability when subsystem "X" is "good" (operating properly), and $R_{SYS,XBad}$ is the system reliability when subsystem "X" is "bad" (failed). Since "X" can be in one of the states (good or bad), but not both simultaneously, they are mutually exclusive.

Each step in the process (assuming successive "Xs" to be "good" or "bad") simplifies the diagram until eventually a series, parallel, or series-parallel model results. At that point, the process can stop. In order to minimize the number of process steps, "X" should be chosen strategically in such a way that the diagram simplifies quickly. In the above example, we begin by considering FMN-202. The reliability of the system can be expressed by the following equation (in the equations that follow, "FMN-XXX" will be abbreviated as "XXX"):

$$R_{\text{RXR}} = R_{\text{RXR+1/1 F nnc}} \cdot R_{1/1} + R_{\text{RXR+1/1 A` c}}(1 - R_{1/1})$$

Finally, factoring and combining like terms yields the following expression for the system reliability, where reliability is defined as successful coverage in the area of FMN-109.

$$\begin{aligned} R_{\text{RXR}} = R_{@}R_{\text{F@SD}}\{&R_{1/1}R_{0/4}R_{0/1}(R_{1/0}R_{0/3}R_{0/2} + R_{0/3}R_{0/2}R_{0/0} \\ &- R_{1/0}R_{0/3}R_{0/2}R_{0/0} + R_{1/3}R_{1/2}R_{1/0}) \\ &+ R_{1/3}R_{1/2}R_{1/1}R_{0/4}R_{0/1}(R_{0/0} - R_{1/0}R_{0/0} - R_{1/0}R_{0/3}R_{0/2} \\ &- R_{0/3}R_{0/2}R_{0/0} + R_{1/0}R_{0/3}R_{0/2}R_{0/0}) \\ &+ R_{1/4}R_{1/3}R_{1/2}R_{1/1}R_{0/1}(R_{1/0} + R_{0/0} - R_{1/0}R_{0/0} \\ &- R_{0/4}R_{0/0} + R_{1/0}R_{0/4}R_{0/0}) \\ &+ R_{1/3}R_{1/2}R_{1/1}R_{1/0}(1 + R_{0/4} + R_{1/4} - R_{1/4}R_{0/4} - R_{0/1} \\ &- R_{0/4}R_{0/1} - R_{1/4}R_{0/1}) \\ &+ R_{0/4}R_{0/3}R_{0/2}R_{0/1}R_{0/0}(1 - R_{1/1})\} \end{aligned}$$

Substituting the reliability values calculated for each assembly yields the following for system reliability, where reliability is defined as successful coverage in the area of FMN-109.

$$R_{\text{RXR}} = 0.986094$$

It should be noted that this probability does not mean that the probability of losing coverage only in the area of FMN-109 is (1 - 0.0986094 = 0.013906). In the model described above, failures leading to the loss of coverage of FMN-109 may also lead to loss of coverage in other areas as well. To calculate the probability of loss of coverage exclusive to FMN-109 would require a different analysis, further illustrating the importance of completely and unambiguously defining the meaning of success, reliability and failure.

Availability

Suppose that this system has an MTBF of 1000 hours. Preventive maintenance, which consists of running system diagnostics, changing filters, and performing visual inspections, is scheduled to take 1 hour and must be done every 200 hours. If a failure occurs, the operators must perform a fault verification test, which requires 1 hour. Diagnostic testing which is performed to isolate the fault to a specific subsystem requires 30 minutes. Once a repair has been identified, approval from management must be obtained before it can be accomplished. The time required to obtain this approval is 4 hours. After the repair has been authorized, the replacement item must be retrieved from stock, which is stored at a remote location, and transported to the system site. This stockroom/travel time requires 36 hours. Repair time, which includes removal of the failed subsystem and installation of a replacement, requires 30 minutes. Once repairs have been completed, a test must be performed to verify that the fault has been corrected. This test requires 1 hour. Finally, management must approve the repair/retest results before the system can be certified to return to on-line status. This approval cycle requires 8 hours.

From the data above, the relevant reliability and maintainability parameters are as follows:

MTBF = 1000 hours
MTBM = 200 hours
Preventive maintenance time = 1 hour
Fault verification test time = 1 hour
Fault isolation time = 30 minutes
Repair time = 30 minutes
Fix verification test time = 1 hour
Time to receive authorization to perform repair (administrative delay) = 4 hours
Time required to retrieve repair unit from stock (logistics delay) = 36 hours
Time to obtain approval that repair has been satisfactorily completed (administrative delay) = 8 hours

Inherent availability is dependent upon MTBF and MTTR, where MTTR considers only fault verification, isolation, repair and repair verification times. From the data above we have:

MTTR = 1.0 + 0.5 + 0.5 + 1.0 = 3 hours

Therefore, inherent availability is calculated as:

$$A_{\text{h}} = \frac{MTBF}{MTBF + MTTR} \times 100\% = \frac{1000}{1000 + 3} \times 100\% = 99.7\%$$

Achieved availability is dependent on MTBM and $MTTR_{Active}$ which includes preventive and corrective maintenance. From the data above, in a 1000-hour time span, the system would be expected to experience 5 preventive and 1 corrective maintenance actions. Therefore, 83.3% of the maintenance activities would be preventive maintenance and 16.7% of the maintenance activities would be corrective maintenance. $MTTR_{Active}$ can then be calculated as a weighted average of the maintenance times.

$MTTR_{Active}$ = (1 hour)(0.833) + (3 hours)(0.167) = 1.334 hours

Achieved availability is then calculated as:

$$A_{\cdot} = \frac{MTBM}{MTBM + MTTR_{@\text{stud}}} \times 100\% = \frac{200}{200 + 1.334} \times 100\% = 99.3\%$$

Operational availability is dependent upon MTBM and MDT. MDT includes $MTTR_{Active}$ and any logistics/administrative delays, which in this case is the time required to receive authorization to perform the

repair, retrieve a repair unit from stock and transport it to the system location, and obtain approval that the repair has been completed satisfactorily. From this data we have:

MDT = (1 hour)(0.833) + (48 hours + 3 hours)(0.167) = 9.35 hours

Operational availability is then calculated as:

$$A_n = \frac{MTBM}{MTBM + MDT} \times 100\% = \frac{200}{200 + 9.35} = 95.5\%$$

RECOMMENDATIONS

These examples reinforce the necessity of properly defining 'success' and 'failure' as accurately and unambiguously as possible. The reliability model and subsequent calculation can vary greatly depending upon these factors. In the examples presented in this paper, the models ranged from simple series to complex, and reliabilities ranged from 88.5% for complete system operability to 98.6% for operability in the area of FMN-109.

It is imperative that reliability modeling and calculations for complex systems be performed by individuals who are skilled in the process and are able to competently analyze the systems. As complex as the reliability math model in the FMN-109 case appears, it should be remembered that it was based upon a scaled down version of the mine. A mesh system covering the entire mine with many cross-links would result in a reliability block diagram and math model significantly more complex than what appears here.

It should be reinforced that many assumptions were made to simplify the reliability block diagram and mathematical models to better illustrate the process. Some of these assumptions include limiting the analysis to the subsystem level with all subsystems being in either a completely working or completely failed state, perfect sensing/switching between the power supply and battery backup for each node, performance of preventive maintenance in accordance with the component manufacturers' recommendations, and ignoring the effect that a catastrophic event may have on the system. A complete reliability assessment should consider failures at the component level, the effects that individual failure modes would have on the system, and the effects of degraded operation. A complete analysis should also consider the impact of catastrophic events and human error on the operation of the system.

As the system grows in complexity, minimum failure paths (referred to as cut sets) that result in system failure become more obscure. In fact, systems that appear to have a great deal of redundancy are sometimes unknowingly subject to single point failures, especially if the paths are not completely independent. In these cases, software can be used to generate the cut sets and aid in the identification of weak areas in the design.

If it is desired to determine the probability of occurrence of a particular failure effect, fault tree analysis (FTA) should be given consideration as an analysis tool. FTA is a systematic top-down approach that begins with the definition of a particular undesired effect and proceeds to determine all of the conditions that could occur that would result in the manifestation of that effect. While Reliability Block Diagrams are oriented toward evaluating the probability of mission success, FTAs are oriented toward evaluating the probability of failure. As with reliability block diagrams, redundancy can be modeled and the probability of occurrence calculated through the use of "OR', 'AND', and voting gates within the Fault Tree.

It can be seen from the availability example that the repair operations have a huge impact on the system. Of course systems should be manufactured to be rugged, but they should balance the ruggedness with quick diagnostics and easy repair with parts that can be kept in stock at the mine operation.

ACKNOWLEDGEMENTS

A major portion of this paper is based on research funded by the National Institute for Occupational Safety and Health (NIOSH), under contract no. BAA-2010-N-12081. The authors would like to acknowledge the discussions and suggestions by David Snyder (NIOSH). Appreciation is also given to the coal companies that have joined the project and have agreed to provide facilities and support during the mine testing phase.

REFERENCES

Nicholls, D ed. 2005. *System Reliability Toolkit*. Reliability and Information Analysis Center, Data and Analysis Center for Software.