911 EMERGENCY PATCH—© ISTOCKPHOTO.COM/LAURAYOUNG,
WOMAN—© ISTOCKPHOTO.COM/HHLTDAVE5

Improving risk assessment in emergency facilities with reliability engineering

CRITICAL OPERATIONS POWER SYSTEMS

BY MICHAEL ANTHONY, ROBERT ARNO, PATRICK SAAD SABA, ROBERT SCHUERGER, & MARK BEIRNE

AT THE REQUEST OF THE U.S. Homeland Security Department in 2005, the National Fire Protection Association (NFPA) developed the first leading practice criterion for building premises wiring in emergency management facilities. These criteria initially appeared in the 2008 National Electrical Code (NEC) as a new section—Article 708: Critical Operations Power Systems (COPS). Article 708 establishes minimum design, commissioning, and maintenance requirements for facilities with engineering documentation that identifies them as designated critical operations areas (DCOAs). One of the key features of Article 708 is the application of quantitative methods for evaluating risk and conveying the results into a power system design that is scaled according to hazards present in any given emergency management district. These methods employ classical lumped parameter modeling of power chain architectures and can be applied to any type of critical facility, whether it is a stand-alone structure, or a portion of stand-alone structure, such as a police station or government center. This article will provide a risk

Digital Object Identifier 10.1109/MIAS.2012.2215993
Date of publication: 3 July 2013

assessment roadmap for one of the most common critical facilities that should be designated as COPS per NEC 708—a 911 call center (the facility that receives and routes the 911 calls to the police or fire departments). The existing methods of reliability engineering will be used in the risk assessment.

Definition of COPS

In October 2005, the NFPA Standards Council issued a directive to the technical correlating committee of the NEC to prepare Article 708 for the 2008 NEC to define a new class of power system. The scope of Article 708 was permitted to extend beyond the NEC's traditional scope, which limited it to the practical safeguarding of persons and property from hazards arising from the use of electricity, further into design, operation, and maintenance criterion [1].

NEC Article 708 defines COPS as "power systems for facilities or parts of facilities that require continuous operation for the reasons of public safety, emergency management, national security, or business continuity." The article also defines DCOA as "areas within a facility or site designated as requiring critical operations power." According to the NEC, COPS are designated by the authority having jurisdiction (AHJ), typically municipal, state, federal, or other codes by any governmental agency having jurisdiction or by facility engineering documentation establishing the necessity for such a system.

The creation of COPS was inspired by the widely perceived need to harden emergency and standby power systems that support homeland security operations. The 9/11 terrorist attacks and Hurricane Katrina revealed the need to reassess national electrical infrastructure protection and reliability at the building premises level, where local practices vary widely. NFPA 1600—*Standard on Disaster/Emergency Management and Business Continuity Programs* contains parallel and complementary requirements that were also updated to better protect critical infrastructure [2]. Underwriters Laboratory Standard 827—*Standard for Central Station and Fire Alarm Systems* also contains criterion for the security of privately owned data centers, but because its criterion is more closely correlated with product-oriented underwriting for insurance companies rather than criterion intended for adoption by organizations involved in the rescue, response, and recovery operations, it will not be covered in this article [3].

As a 911 call center is the critical communications link between the public and both the police and fire departments, the authors of this article have assumed that most, if not all, local emergency management agencies would require that 911 call centers be engineered, built, commissioned, and maintained according to Article 708 requirements.

NEC Article 708 Overview

Article 708, Section I—General contains the following elements:

- 708.1 Scope
- 708.2 Definitions
- 708.3 Application of Other Articles
- 708.4 Risk Assessment
- 708.5 Physical Security
- 708.6 Testing and Maintenance 708.8 Commissioning

The other sections in Article 708 are as follows:

- Section II—Circuit Wiring and Equipment
- Section III—Power Sources and Connection
- Section IV—Overcurrent Protection
- Section V—System Performance and Analysis.

This article will focus primarily on 708.4 Risk Assessment to provide typical techniques used in reliability engineering and show how it can be used to evaluate the reliability and scale the availability of the COPS. Some of the other sections, such as the section on overcurrent protection, also have an impact on reliability. Because of the space constraints, the analysis in this article assumes proper selective coordination of all overcurrent protective devices, which is an important factor.

Risk Assessment

A key concept of COPS engineering appears in Section 708.4:

> Risk Assessment for COPS shall be documented and shall be conducted in accordance with 708.4(A) through (C)
>
> (A) Conducting Risk Assessment—Identify hazards, the likelihood of their occurrence and vulnerability of the electrical system to those hazards.
>
> (B) Identification of Hazards—Minimum shall include, but shall not be limited to, the following:
>
> 1) Naturally occurring hazards (geological, meteorological, and biological).
>
> 2) Human-caused events (accidental and intentional).
>
> (C) Developing Mitigation Strategy—Based on the results of the risk assessment, a strategy shall be developed and implemented to mitigate hazards.

There are a number of methodologies and techniques available for risk assessment that range from simple to complex [4], [5]. The major categories of techniques are listed as follows: the what-if, checklist, what-if/checklist, hazard and operability study, and failure modes, effects, and criticality analysis (FMECA) techniques provide qualitative results; fault-tree analysis (FTA) can be used to provide both qualitative and/or quantitative results; and reliability block diagrams (RBDs) provide primarily quantitative results.

What-If

The purpose of the what-if analysis is to identify specific hazards or hazardous situations that could result in undesirable consequences. This technique has limited structure but relies on knowledgeable individuals who are familiar with the areas/operations/processes. The value of the end result is dependent on the team and how thorough they are in raising questions regarding potential hazards.

Checklist

In a checklist analysis, a specific list of items is used to identify hazards and hazardous situations by comparing the current or projected situations with accepted standards. The value of the end result is dependent on the quality of the checklist and the skill and understanding of the checklist user.

What-If/Checklist

The what-if/checklist analysis is a combination of the what-if and checklist techniques that utilizes the strength of both

methods to complete the risk assessment. The what-if questions are developed and the checklist(s) used to encourage the creativity of the what-if process as well as to fill in any gaps in the process of developing questions. The value of the final result is dependent on the team and how thorough they are in raising questions regarding potential hazards.

Hazard and Operability Study

A hazard and operability study requires an interdisciplinary team that is very knowledgeable about the areas/operations/processes to be assessed. This approach is thorough, time consuming, and costly. The value of the final result depends on the skill and understanding of the team, the quality of the reference material available, the ability of the team to function as a team, and the presence of strong, positive leadership.

Failure Modes, Effects, and Criticality Analysis

In an FMECA, each element in a system is examined both individually and collectively to determine the effect when one or more elements fail. This is a bottom-up approach: each of the elements is examined, all of the ways it can fail are listed (failure modes), and the effect of each failure to the element itself and on the overall system is predicted. Then, a criticality level is assigned for each failure mode based on the overall effect on the system. An interdisciplinary team is required, and it is time consuming in direct proportion to how thorough and to what level of detail the analysis is conducted. This technique is useful for assessing potential equipment failures and how they impact the overall mission of the system being analyzed. The value of the final result is dependent on the skill and understanding of the team and the scope of the analysis performed.

Fault-Tree Analysis

FTA is a top-down approach in which an undesirable event is identified as the top event in the tree, with the potential causes that could lead to the undesirable event identified as branches below. Boolean algebra is used to connect the potential causes of failure in the branches to other branches and to the top event. If the failure rate (FR) and repair data are available for all of the initiating failures in the fault tree, quantitative results (unreliability and unavailability) can be calculated for the top event and each of the branches. The value of the assessment is dependent on the team's competence in using the FTA process, skill and understanding of the systems it is analyzing, and the depth to which it conducts the analysis.

Reliability Block Diagram

An RBD is a block diagram in which the major components are connected together in the same manner as they are in a lumped parameter one-line or piping diagram. Each of the blocks has the failure and repair data for that component included in the block. The junctions connecting the blocks are set according to the system redundancy (e.g., one out of two when there are two components and only one is required to carry the load). Quantitative results (reliability, availability, and so forth) for the RBD are obtained by performing the series and parallel combinations of the blocks.

Risk Assessment of COPS

Risk assessment for COPS is performed to identify hazards, the likelihood of their occurrence, and the vulnerability of the COPS to those hazards. These hazards include equipment failure, inclement weather, flooding, earthquakes, and civil disturbances (see NFPA 1600 Appendix 5.3 for a more comprehensive list of potential vulnerability parameters). This assessment could be called a vulnerability analysis. From the vulnerability analysis, the power distribution architecture and supporting mechanical systems can then be properly selected to achieve the desired reliability [6].

It is noteworthy that the hazards listed in 708.4(B) are not just items that could cause the electrical system to fail. Obviously, electrical systems are immune to biological hazards. NFPA 1600-2007—*Standard on Disaster/Emergency Management and Business Continuity Programs* can be used as a model for Article 708 and is referenced in many places. Therefore, the risk assessment should be comprehensive and look at all of the major hazards that would take the 911 call center out of service.

For our example 911 call center, we use a very robust design in which there are two complete systems for each part of the critical infrastructure. In the data center world, this is referred to as 2*N*, in which *N* is the number (needed). The critical systems are as follows:

1) electrical power (ac)
2) electrical power (dc)
3) mechanical cooling system
4) telephone system
5) shortwave radio system
6) IT systems including Internet connection
7) building life safety systems (structural and fire protection).

Figure 1 shows the one-line diagram for our example facility. The IT equipment, shortwave radio, and mechanical cooling systems are on ac power. The telephone system uses dc power.

Figure 2 shows the mechanical cooling system. It is also 2*N*, with one air-cooled chiller and one water-cooled chiller. The water-cooled chiller is more economical to operate but requires water to make up for evaporation from the cooling tower. The air-cooled chiller can operate without make-up water should the city water supply be lost.

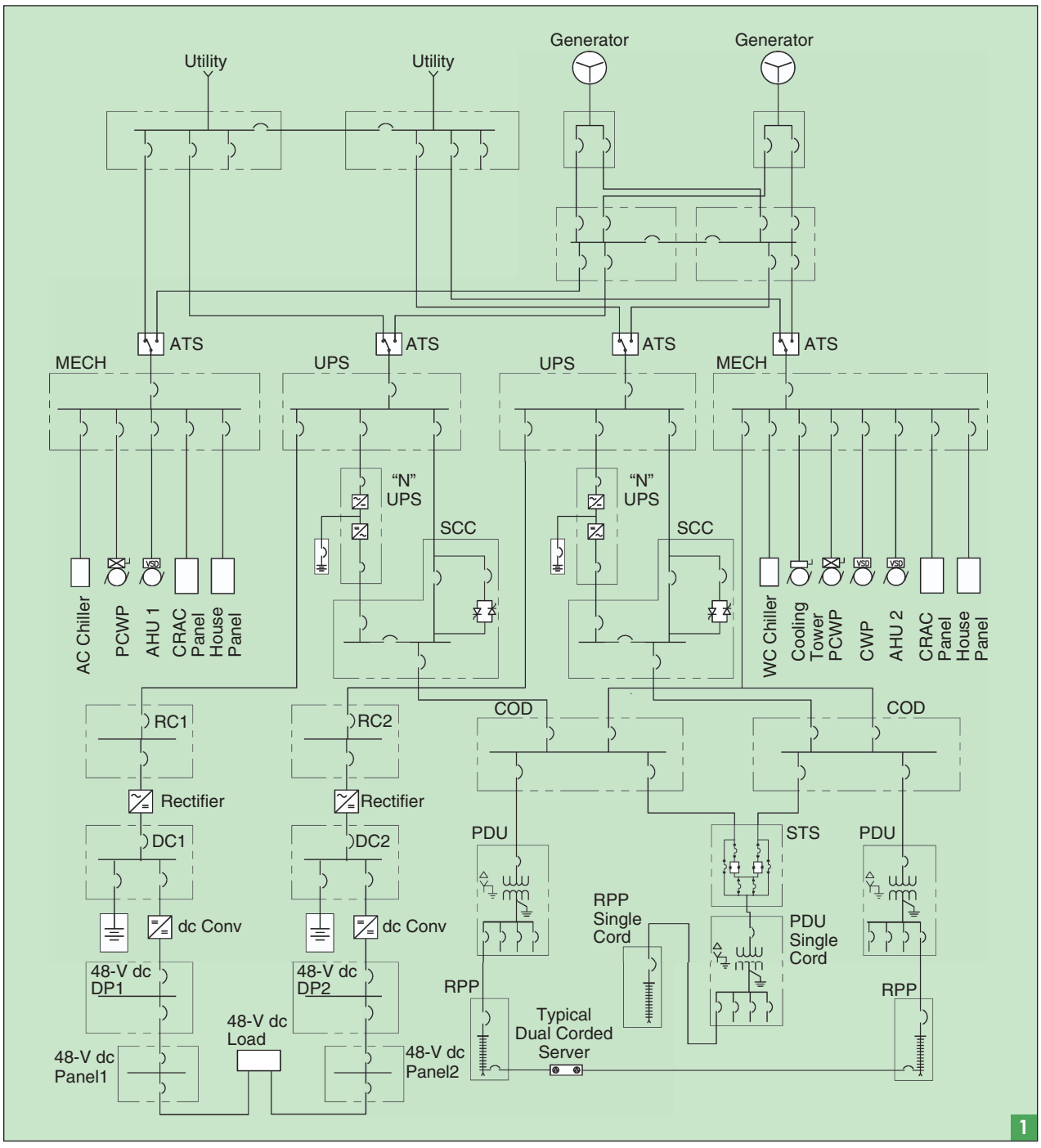
Control systems play a major role in determining the reliability of critical facilities and should be considered the third component to electrical and mechanical systems. The complexity of the control systems varies based on the size and complexity of the facility. For this reason and for a better understanding of this application, control systems were not included.

Annex F

Because many of the concepts underlying Article 708 cannot be crafted in mandatory legislative language, an Annex F was included in the 2008 NEC to familiarize the premises wiring safety community, the bulk of the users of the NEC, with some of the vocabulary of reliability engineering. Annex F also highlights the importance of proper installation and commissioning of COPS.

Availability and reliability are defined in Annex F as follows:

- Availability: the percentage of time a system is available to perform its function.



The one-line diagram of the 911 call center.

- Reliability: the probability that an item can perform its intended function for a specified interval under stated conditions.
- Maintainability: a measure of how quickly and economically failures can be prevented through preventive maintenance or system operation can be restored following failure.

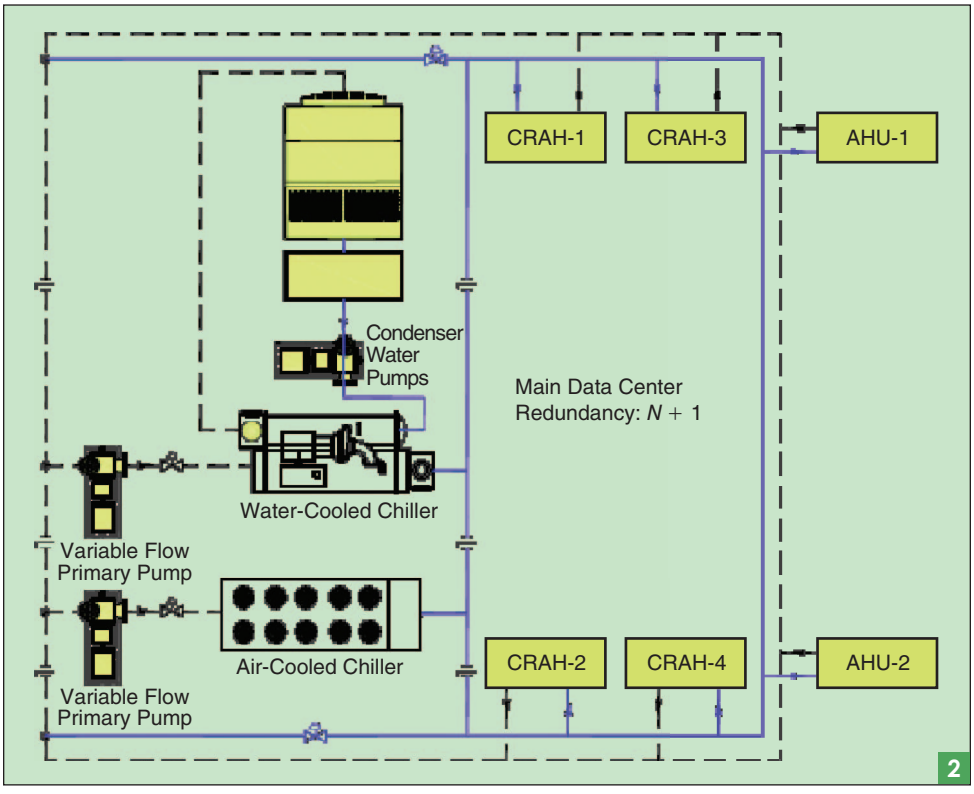
Availability is calculated by

$$A = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}},$$

where mean time between failures (MTBF) is the average time the equipment performed its intended function between failures, and mean time to repair (MTTR) is the average time it takes to repair the failure and put the equipment back into service.

Reliability Analysis

IEEE Gold Book (Standard 493-2007)—*Recommended Practice for Design of Reliable Industrial and Commercial Power Systems* [7] provides the methodology and failure and repair data required to perform reliability analysis on electrical



The cooling system for the 911 call center.

and mechanical systems. (Space does not permit listing the actual data used.) The method used in the *IEEE Gold Book* is RBD. RBD is an effective method for analyzing systems with many interrelated items, such as an electrical distribution system.

For simple systems that consist of series and parallel blocks, the calculations can be performed manually. For complex systems with standby components, such as the system shown in Figure 1, reliability software is needed. Table 1 shows the reliability analysis for Figures 1 and 2, using reliability software to calculate the reliability, availability, MTBF, and MTTR for each.

There is a significant difference between what is considered a failure for electrical power to the critical ac loads and dc telephone systems when compared to failure for power to the mechanical cooling systems. Momentary loss of power to the critical ac loads and telephone systems is considered a failure, as the uninterruptible power supply (UPS) system and the 48-V dc systems have batteries to provide power while the generators start (during loss of utility power). For the electrical power to the mechanical cooling systems, momentary loss of power is not considered a failure, as the mechanical cooling system is designed to go down and restart.

There is also a significant difference between loss of power to the critical ac and dc loads and loss of cooling. Loss of power to the critical ac load or telephone system causes an immediate failure. Loss of cooling does not. The equipment has to overheat before it shuts down, which may take a significant amount of time.

The reliability analysis shown for the mechanical cooling system shows only the reliability of the equipment itself. It does not address the probability that any equipment will actually overheat.

The COPS must operate for a long period of time, providing power to systems that perform critical functions. Section 708.22(C) specifically requires that the alternate power source is capable of operating 72 h at full load. Therefore, the 911 call center would require significant onsite diesel fuel storage to be included in the design.

Additional Tools for the Risk Analyst

Annex F of NEC 2008 also provides direction on how to improve the availability of COPS, both for existing and new facilities. The methodology includes the reliability analysis of evaluating possible failures of the system by conducting an FMECA and/or an FTA. Because of the complexity of the modeling and interpretation of the risk analysis, Annex F references supporting documents.

The Army Corp of Engineers Power Reliability Enhancement Program (PREP) training manual *TM 5-698-4—FMECA for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities* provides the necessary information on the how to conduct an FMECA [8].

TABLE 1. RELIABILITY ANALYSIS FOR CRITICAL ELECTRICAL AND MECHANICAL SYSTEMS (FR = FAILURES/H OF OPERATION).

Description of RBD	FR	MTTR (h)	Availability	Reliability (Five Years) (%)
Electrical power for critical ac loads	2.1464 E-06	6.31	0.9999865	7.70
Electrical power for critical dc loads	2.4037 E-06	5.92	0.9999858	9.03
Electrical power for mechanical system	5.4260 E-07	2.19	0.9999988	4.30
Mechanical cooling system	2.7977 E-07	7.15	0.9999980	1.46

As the name states, an FMECA is the process of looking at all of the failure modes for the equipment or system being analyzed and determining what effect each failure would cause. There can be more than one effect, and it is normal to list them as primary, secondary, and so forth.

As a simple example, a molded case circuit breaker has the following major failure modes:

1) failure to open when it should
2) failure to close when it should
3) failure to conduct or stay closed when it should.

The "when it should" part of each failure mode creates a further breakdown of each. For example, the first (fail to open) might occur for a number of reasons, such as the following:

1) The thermal unit is defective and did not detect the overload.
2) The instantaneous (magnetic) element is defective and did not detect the short circuit.
3) The mechanism is defective and pulling the handle did not separate the contacts.
4) The contacts are welded shut from a previous failure and cannot be opened even manually.

IEEE Standard 3007.2-2010—*Recommended Practice for the Maintenance of Industrial and Commercial Power Systems* also has a detailed example of an FMEA for a 480-V switchboard that demonstrates this process [9].

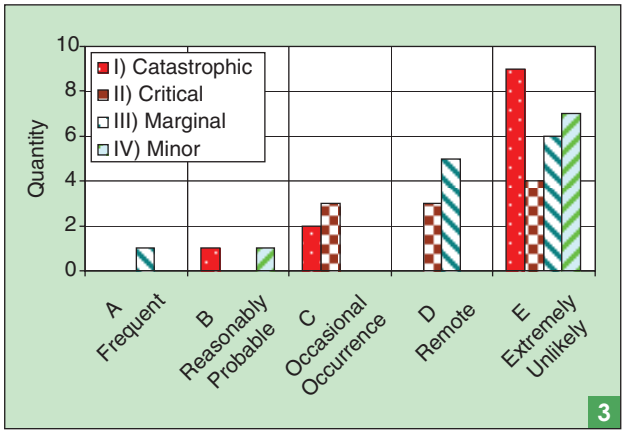
The FMECA process is continued until all of the major failure modes for all of the equipment (or systems) being evaluated have been listed out. Then, the primary, secondary, and other effects are listed for each failure of each piece of equipment. In our example, assume that the circuit breaker was supplying a motor that pumped chilled water to the computer room air handling (CRAH) units. The primary effect of the circuit breaker not tripping could be that the motor keeps running and starts a fire (if it has a short circuit and the breaker upstream does not clear the fault), or the whole cooling system might pass down when the main breaker trips to clear the fault. The secondary effect may be the loss of some of the IT equipment being cooled by the CRAH units, which in turn may create further effects. If the cooling system has been designed with redundancy, there may be no secondary effects, as loss of one pump might not cause any IT equipment to overheat. If a fire starts, it might force the whole raised floor IT load to go down regardless of the cooling system.

Once all the failure modes and effects have been defined, the next step is to look at the criticality of the effects in conjunction with the probability of each one happening. The normal method is to have a gradient scale of criticality like the following example:

1) catastrophic: major human injury, significant financial loss, and significant PR impact
2) critical: significant loss of production and minor human injury
3) marginal: minor loss of production
4) minor: no significant impact on production

The probability of each failure is then addressed. Another gradient scale is often used, such as the following:

1) frequent
2) reasonably probable
3) occasional occurrence
4) remote
5) extremely unlikely.



The FMEA criticality matrix.

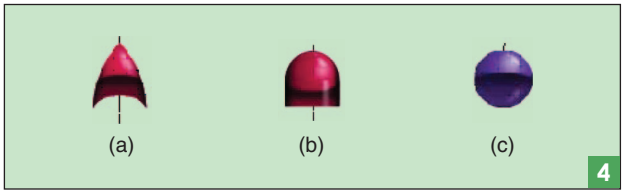
Each failure and its associated effect is then evaluated in terms of criticality and likelihood of occurrence and put into a matrix, as shown in Figure 3.

If a system has been very well designed, no catastrophic events are likely to occur. Often the point of doing the FMECA in the first place is to evaluate how well the system has been designed. The FMECA matrix points out which areas need to be addressed that will have the biggest impact on the overall operation of the system. It also shows which areas not to bother with, as either the hazards are extremely unlikely to occur or the effect when they do occur is minor.

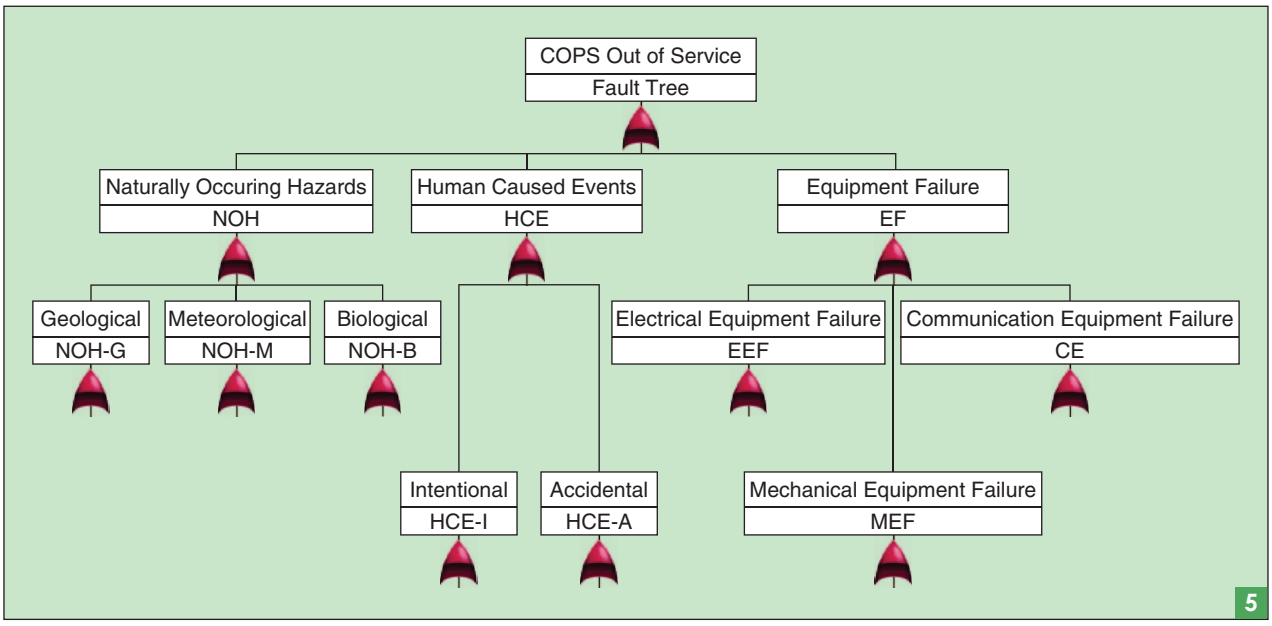
To perform a risk assessment using FTA, the event to be investigated is placed at the top of the tree. Below the top event are the items that can cause the top event to occur. The fault tree uses Boolean algebra, with OR gates (in which either event can cause a failure), AND gates (which require both events for the failure), and initiating events (which are events like equipment failures to be evaluated) (Figure 4).

Figure 5 shows the top part of a fault tree for COPS that can be used to perform a risk assessment. The top event is COPS out of service. The hazards listed in Section 708.4—Naturally Occurring Hazards and Human Caused Events have been diagrammed, with the addition of the equipment failure as an additional source of the COPS out of service. Equipment failure could have been included under human-caused events. It is, however, an item that can be specifically addressed with reliability analysis much more easily than other types of human-caused events, such as operator error.

Below each of the major hazards, additional parts of the fault tree would be included. Figure 6 shows the expansion of the communications equipment failure. If the telephone system fails, communication with the outside world is lost (CO = central office for telephone company). If the short-wave radio system is lost, communication with the police



The fault-tree symbols: From left: (a) OR, (b) AND, and (c) initiating event.



The fault tree for the COPS.

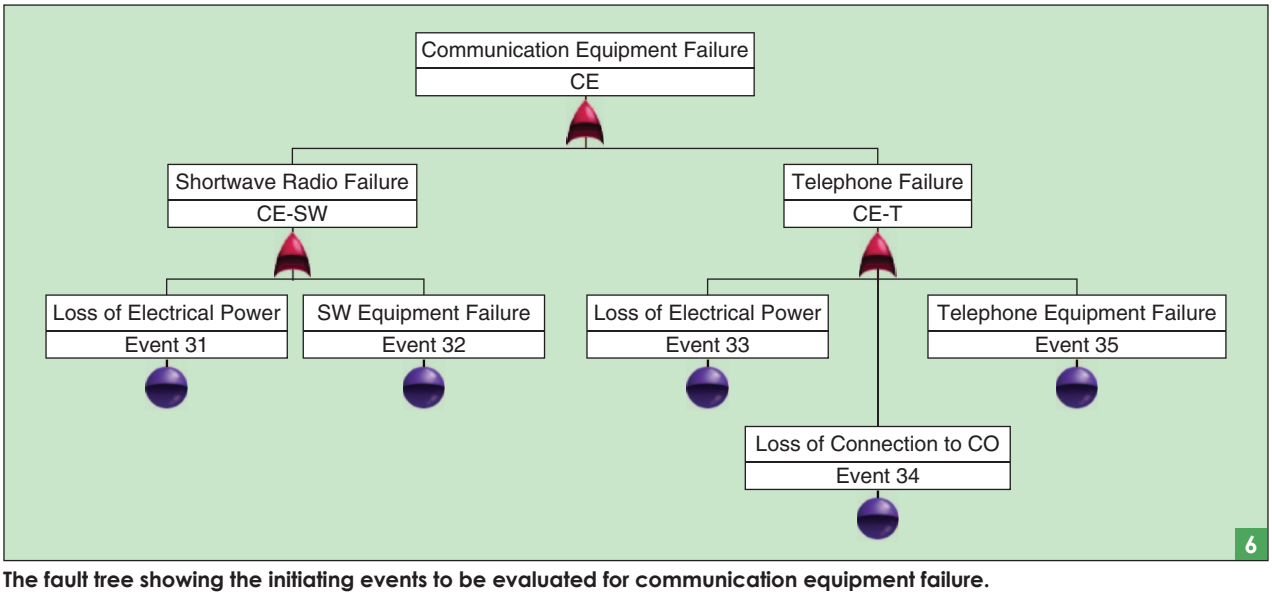
and firefighters in the field is lost. Some 911 call centers may also consider loss of Internet communication a critical failure, but for this example, we assumed that the center could continue to function without it.

This diagram shows all of the initiating events that will be evaluated in the fault tree. The rate at which past failures have occurred (FR) for each of the initialing events would be listed in that figure. For example, Table 1 shows the FRs for loss of ac or dc power to the shortwave radio or telephone system, respectively.

Once all of the FRs have been determined for all of the initiating events, the fault tree can be calculated and the reliability and availability of the fault tree determined. Obtaining an FR for some of the items would be relatively easy, as the *IEEE Gold Book* provides data on a wide range of electrical and mechanical equipment.

However, for some of the items, such as infectious agents under biological hazards, it would be much more difficult to determine an FR. Human-caused failures, whether intentional (sabotage) or accidental, are also very difficult to quantify. In areas where failure data is not available, direct reliability and availability analysis cannot be performed. Mitigation strategies, such as security systems and preventing access to the COPS or their support systems, will have to address these types of issues without the assistance of reliability analysis.

Reliability analysis can be done using several different methods. FTA is quite effective in analyzing a system in which a number of factors (that are relatively independent of each other) can cause a system failure. It is also very useful in showing the relationships between the systems.



The fault tree showing the initiating events to be evaluated for communication equipment failure.

Even with the best engineering design and technology, it may be economically impractical and technically impossible to design, build, and maintain COPS that will never fail over a long period of operation. Forced outages can and do occur, which is why the original authors of Article 708 included COPS maintenance and commissioning requirements of Sections 708.6 and 708.8 in the enforceable text of the NEC.

When forced outages do occur, restoring the COPS to operation as quickly and economically as possible is very important. Thus, the maintainability characteristics of the COPS facility will predict how quickly and economically they will be restored to normal operation. This is why reliability, availability, and maintainability are considered complementary characteristics [10], [11].

Conclusions

Article 708 leaves much to the judgment of the engineer designing the COPS. The quantitative approaches described in this article will lead to more consistency in those judgments by conveying opinions about power security into the realm of science. The risk assessment method chosen to analyze the COPS should be correlated with the hazards in any given emergency management district and should be appropriate for the system in question. It should require only a reasonable level of investment given the value of the results. The failure of some components may have little impact on either system function or its operating repair costs. Given the ranking of hazards in any given emergency management district and the subtlety in the performance of the power chain architecture, a relatively costly analysis may not be justified.

In any case, when the consequences of failure are catastrophic, every possible effort should be made to make the COPS fail safe. An appropriate risk assessment is one that economically directs the local emergency management agencies on how to best spend the limited funds they have on the most effective upgrades to the facilities.

Article 708 was added to the NEC Special Conditions chapter when the NFPA realized the need and the means to convey the best practices of the business continuity industry into the public sector emergency preparedness. In general, building codes (NFPA 101, NFPA 5000, IBC, and so forth) tend to mandate requirements that contribute to public safety and, to a lesser extent, property protection. Article 708 and its optional supporting material present a performance-based design approach that is better suited for the spectrum of COPS facilities and their diverse users.

There are still significant jurisdictional issues to be worked out before Article 708 conformity becomes the main driver for increased homeland security funding at the building premises level [12]. The wisdom in placing COPS requirements into the NEC is that its presence would instantly be discussed in building departments among local authorities having jurisdiction and emergency management functionaries. It has requirements that are clearly outside the scope of the normal practice of building premises wiring. Other documents, such as NFPA 1600—*Standard on Disaster/Emergency Management and Business Continuity Programs* and NFPA 110—*Standard for Emergency and Standby Power Systems*, will have to be revised to align and support the intent of COPS.

Looking forward to future revision cycles of the NEC, a logical next step would be to define scalable levels of COPS to match the different levels of criticality of the various types of facilities. For example, a facility required to provide emergency communication across a large area, such as a 911 call center, is more important to public safety than an individual police or fire station. Therefore, the 911 call center should have more robust COPS than what would be necessary for the individual police or fire station. The AHJ should also be provided with some guidelines for assessing acceptable reliability and availability for the various types of facilities critical to homeland security.

It is noteworthy that the analysis presented in this article is based on the 911 call center being the only source of support for the region in which it operates. If there are multiple 911 call centers covering the same region, the risk assessment should include the effects of back-up centers or redundant centers providing duplicate services.

References

[1] J. Lardear, *When Failure Isn't an Option*, NEC Digest Standard, Feb. 2007.

[2] *Standard on Disaster/Emergency Management and Business Continuity Programs*, NFPA Standard 1600.

[3] *Standard for Safety Central Station Alarm Services–Underwriter's Laboratories*, UL Standard 827.

[4] M. A. Anthony, *Consulting-Specifying Engineer*, NEC Standard 708, May 2007.

[5] M. A. Anthony, R. G. Arno, and E. Stoyas, "Article 708: Critical operations power systems" *Elect. Construction Maintenance Mag.*, vol. 106, no. 11, p. 64, Nov. 2007.

[6] M. A. Anthony, R. Arno, R. Schuerger, and E. Stoyas, "Risk assessments for critical operations power systems," *Pure Power Mag.*, June 2008.

[7] *Recommended Practice for Design of Reliable Industrial and Commercial Power Systems*, IEEE Standard 493, 2007.

[8] *Failure Modes and Effects Criticality Analysis (FMECA) for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities,* Army Corp of Engineers Power Reliability Enhancement Program (PREP) Training Manuals TM 5-698-4, 29 Sept. 2006.

[9] *Recommended Practice for the Maintenance of Industrial and Commercial Power Systems*, IEEE Standard 3007.2, 2010.

[10] R. Arno, R. Schuerger, and E. Stoyas, "Article 708, critical operations power systems—Some existing technologies to assist in complying," *IAEI Mag.*, Nov.–Dec. 2008.

[11] R. Arno, R. Schuerger, and E. Stoyas, "Risk analysis for NEC article 708 critical operations power systems," in *Proc. IEEE IAS Conf.*, 2009, pp. 1–7.

[12] M. A. Anthony and R. Aaron, "Critical operations power systems: Success of the imagination," *Int. City-County Manage. Mag.*, vol. 91, no. 1, p. 7, Jan.–Feb. 2009.

Michael Anthony is with the University of Michigan, Ann Arbor. Robert Arno, Patrick Saad Saba, and Robert Schuerger (bschuerger@hp.com) are with HP Critical Facility Services in Bethesda, Maryland. Mark Beirne is with DLB Associates in Chicago, Illinois. Anthony, Arno, and Schuerger are Senior Members of the IEEE. This article first appeared as "Reliability Engineering Applied to Critical Operations Power Systems (COPS)" at the 2011 IEEE IAS Industrial and Commercial Power Systems Technical Conference.