ANSWERING SUBSTATION AUTOMATION QUESTIONS THROUGH FAULT TREE ANALYSIS

Gary W. Scheer
Schweitzer Engineering Laboratories, Inc.
Pullman, WA USA

ABSTRACT

Substation automation designers are faced with many choices about system topology, primary and backup devices, and redundant data paths. Determining the reliability of substation automation systems can be a significant analytical problem. The paper includes examples that illustrate practical applications of fault tree analysis to compare the relative reliability of system configurations. The paper shows that fault tree analysis is a practical tool to help understand and answer integration questions.

INTRODUCTION

In the 1970s and 1980s engineers had many choices of vendor equipment for substation instrumentation and control. Regardless of the supplier, virtually all remote control and indication systems included a remote terminal in the substation as the SCADA connection. Engineers were primarily concerned with reliability at master control centers, where dual systems were often employed in response to almost daily failures of early magnetic media, computers, and monitors.

Today designers can choose a wide variety of devices and methods to form an overall instrumentation and control system**.** In many cases microprocessor-based protective relays were installed for line protection. Designers now recognize a potential cost savings by having the equipment provide "double duty" as a part of the SCADA system.

Some of the factors that a designer considers in selecting the I&C components and designing the system are equipment costs, installation and commissioning costs, performance, security, vendor independence, and reliability. This paper is concerned with the reliability component of the selection and design process.

Reliability engineers have developed many tools to analyze the failure states and probable failures of systems**.** In the electric utility industry, engineers involved in nuclear power plant design may be familiar with a variety of tools and computer programs employed to assess critical system reliability. Some engineers exposed to failure analysis of large systems note the expenditure of effort and degree of complexity in those analyses; thus, they may feel that they cannot justify the time to learn the methods and computer programs for such an analysis. This paper provides a substation I&C designer with tools to compare the reliability of systems without expending days of training in theory, methods, or computer applications programs. Any of the examples in this paper can be calculated in a few minutes with a hand-held calculator.

In an earlier paper [1], colleagues applied fault trees to analyze transmission protection. With their permission, this paper quotes their background text, below:

"Since reliability is the reciprocal of failure, and failure is a random event, probabilistic measures are most appropriate, and we apply the laws of probability theory.

For example, suppose the reliability of a device is expressed with a mean-time-between-failure (MTBF) of 100 years. The failure rate is 1/100 failures per year. And, if a system has 300 of these devices, then we would expect $300 \cdot (1/100) = 3$ device failures per year.

We use the method of combining component failure rates called "fault tree analysis," a concept first proposed by H. A. Watson of Bell Telephone Laboratories to analyze the Minuteman Launch Control System. This method, used and refined over the ensuing years [2], is attractive because it does not require extensive theoretical work and is a practical tool that any designer can learn to use. While computer programs are available to assist in developing and analyzing complex fault trees, this paper shows that small fault trees, which are easily analyzed manually, are also very useful.

If a device consists of several components, then a fault tree helps us combine component failure rates to calculate the device failure rate. Refer again to our device which has a failure rate of 1/100 failures per year. It might consist of two components, each with a failure rate of 1/200 failures per year. Both components must operate properly for the device to be sound. The individual failure rates of the two components add up to the total failure rate of 1/100. We add the component failure rates to obtain the device failure rate if either component can cause the device to fail.

On the other hand, our device with the 1/100 failure rate might consist of two redundant components each with a failure rate of 1/10 failures per year. Either component can give satisfactory performance to the device. The product of the individual component failure rates is the device failure rate. We multiply component failure rates to obtain the device failure rate if both components must fail to cause a device failure." [1]

Designers can use fault trees to determine the failure rate of a combination of components. Failure rates are useful for estimating maintenance costs but do not adequately indicate whether a device will be available when needed. This paper also shows how to calculate estimated unavailability, which is the fraction of time a device cannot perform. Given the unavailability of the components in a system, fault trees are useful to determine the predicted unavailability of the system.

DEVICE FAILURE RATES AND UNAVAILABILITIES

The device failure rate provides the number of failures expected per unit of time. It is common to express failure information as the Mean Time Between Failures (MTBF). By strict definition, MTBF is the sum of the Mean Time To Fail (MTTF) plus the Mean Time to Repair (MTTR). Compared to the MTBF the repair time is quite small, so this paper approximates the MTBF to be equal to the MTTF.

Availability and unavailability are often expressed as probabilities [4]. For these examples, all of the failure rates are based on field data, or assumptions that devices of comparable complexity and exposure will have similar failure rates.

Reference 2 describes how to calculate unavailability given a failure rate and the time it takes to detect and repair a failure.

$$q \cong \lambda T = \frac{T}{MTBF}$$

where: q is unavailability
λ is some constant failure rate
T is the average down-time per failure
$MTBF = \frac{1}{\lambda}$ is Mean Time Between Failures.

Each failure causes downtime T. Therefore the system is unavailable for time T out of total time MTBF. The fraction of time the system is not available is therefore $\frac{T}{MTBF}$ [1][2].

Personal Computer Hardware

Industry trade publications vary in reporting the MTBF of personal computers. Generally, an MTBF of 22,500 hours seems typical for a "good quality PC or clone." Assume that a problem will be detected and repaired within 48 hours. The unavailability is

$$q = \left(\frac{48 \text{ hours}}{22{,}500 \text{ hours}} \right) = 2133 \cdot 10^{-6}$$

$$q \cong 2130 \cdot 10^{-6}$$

Industrial "Rugged" Personal Computer Hardware

A typical manufacturer of industrial Personal Computers quotes an MTBF of 125,000 hours. Assume once again that a problem can be detected and repaired in 48 hours. The unavailability is

$$q = \left(\frac{48 \text{ hours}}{125{,}000 \text{ hours}} \right) = 384 \cdot 10^{-6}$$

$$q \cong 385 \cdot 10^{-6}$$

You can further improve the availability of the industrial PCs by selecting redundant options for the highest failure prone components of the PC.

Remote Terminal Unit (RTU)

For the small substation example, I used the 100,000 hour MTBF published by two RTU vendors for the appropriate size of RTU. For a larger system, you would analyze the RTU system components to determine the appropriate unavailability. For the examples, the unavailability is

$$q = \left(\frac{48 \text{ hours}}{100{,}000 \text{ hours}} \right) = 480 \cdot 10^{-6}$$

$$q \cong 480 \cdot 10^{-6}$$

Transducer

Data from transducer vendors shows an MTBF of 76 years. Assume a mean-time to detect and repair of 48 hours

$$q = \left(\frac{48 \text{ hours}}{76 \text{ years} \cdot 365 \text{ days / year} \cdot 24 \text{ hours / day}} \right) = 72 \cdot 10^{-6}$$

$$q \cong 70 \cdot 10^{-6}$$

Programmable Logic Controller (PLC)

The nuclear and process industries have evaluated PLC failure rates. Data from references 4, 5, and 6 yields an MTBF of 17 years for PLCs from a variety of manufacturers. Assume that a failure can be detected and repaired within 48 hours; the unavailability is

$$q = \left(\frac{48 \text{ hours}}{17 \text{ years} \cdot 365 \text{ days / year} \cdot 24 \text{ hours / day}} \right) = 322 \cdot 10^{-6}$$

$$q \cong 320 \cdot 10^{-6}$$

Since industrial computers and PLCs are similar in many ways, it is reassuring that independent data sources yield comparable unavailabilities.

Substation Communications Processor

Data from a manufacturer's experience shows an MTBF of 200 years for a communications processor designed for a substation environment. Again assume 48 hours to detect and repair a failure; the unavailability is

$$q = \left(\frac{48 \text{ hours}}{200 \text{ years} \cdot 365 \text{ days / year} \cdot 24 \text{ hours / day}} \right) = 27 \cdot 10^{-6}$$

$$q \cong 30 \cdot 10^{-6}$$

Protective Relay as Data and Control Component

References 1 and 3 provide an unavailability for microprocessor-based protective relays of

$$q \cong 100 \cdot 10^{-6}$$

When relays are connected in a multidrop network, some failure modes can corrupt all communications on the network. Assume that of all relay failures, only 20% prevent communications between other devices. The unavailability of the network due to the "network failure mode" of a relay is therefore

$$q \cong 20 \cdot 10^{-6}$$

Network Repeater

Assume that a network repeater has complexity on the order of a rugged PC. By similarity, assume an unavailability of

$$q \cong 385 \cdot 10^{-6}$$

Assume that under 20% of the repeater failures will prevent other devices on the network above the repeater from communicating. The "network failure mode" of the repeater will impact network unavailability as follows:

$$q \cong 70 \cdot 10^{-6}$$

Table 1: Approximate Unavailabilities of Several Components

Component	Unavailability
Described in This Paper	
Personal computer	2135×10^{-6}
Industrial personal computer	385×10^{-6}
Medium remote terminal unit	480×10^{-6}
Transducer	70×10^{-6}
Programmable logic controller	320×10^{-6}
Substation communications processor	30×10^{-6}
Protective relay hardware	100×10^{-6}
Protective relay multidrop network failure	20×10^{-6}
Network repeater	385×10^{-6}
Network repeater multidrop network failure	70×10^{-6}
From Reference 1	
Circuit breaker	300×10^{-6}
Leased telephone line	1000×10^{-6}
DC power system	50×10^{-6}
Modem	30×10^{-6}
Simple fiber-optic transceiver	10×10^{-6}
Current transformer (per phase)	10×10^{-6}
Voltage transformer (per phase)	10×10^{-6}

Tabulating component unavailability allows you to quickly see which components are most likely to cause problems. A column showing component price could be added to shed early light on the economics of the quality problem. I used representative data to determine unavailabilities to illustrate the fault tree analysis. When comparing two real alternatives, you will be best served by using field failure rates and down-time information instead of these representative examples.

FAULT TREE CONSTRUCTION EXAMPLE

A fault tree is used to determine the probability of a particular failure of interest. It models the part of the system that influences the particular failure. The "failure of interest" is called the Top Event. Consider the example of a remote terminal unit in a substation with six lines and six breakers, as shown in Figure 1.

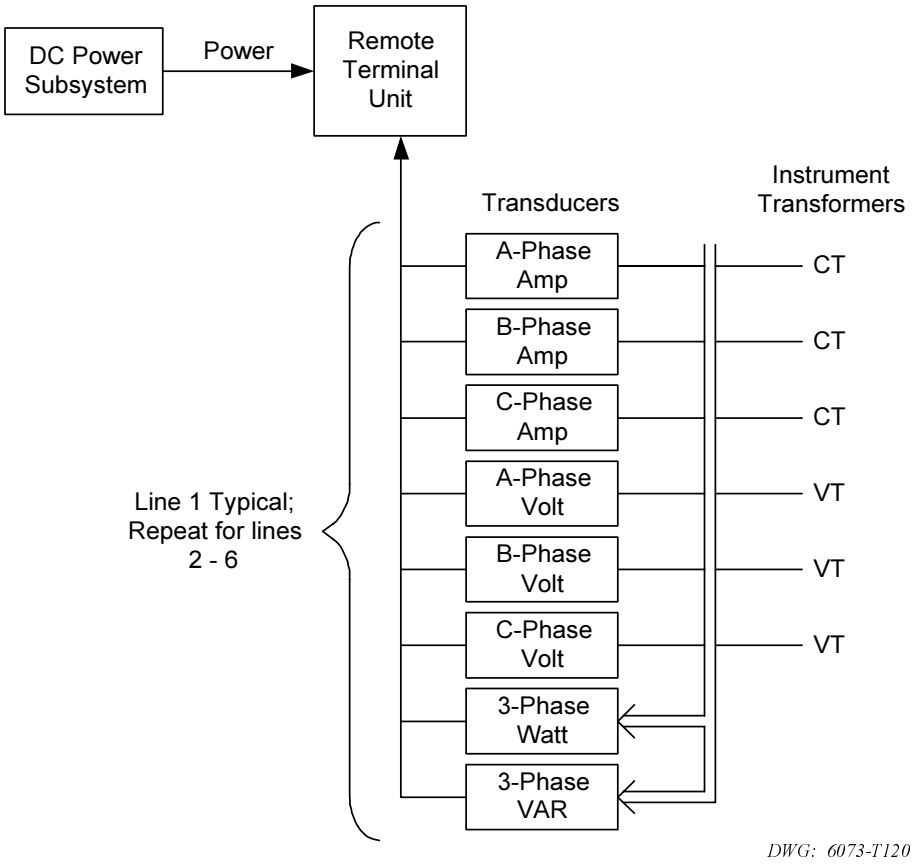

Figure 1: Example RTU System for a Six-Line Substation

For this example, suppose you are interested in the probability that the analog data for Line 1 will fail to be available to a master station. Summarize the top event in a box at the top of the fault tree. Use the fault tree to break the top event into lower-level events. The OR Gate in Figure 2 expresses the idea that any of several failures can cause the top event. Lower-level events can be basic events, which are depicted with a circle and referred to as "roots." The roots are failures of devices such as the leased line, modem, instrument transformers, or the DC subsystem. If we have a reasonable unavailability for the device, no further analysis of the device is required. A lower-level event can instead be the result of combining other lower-level events to determine the unavailability. These events are depicted with boxes.

It is important to identify all causes of the event, inside and outside of the part of a system you are evaluating. This discipline helps you find opportunities to improve overall reliability and helps you calibrate the contribution of alternatives relative to other common failure causes. Use OR gates to combine multiple events, when any one failure will result in the failure of the event above the gate. Use AND gates to combine multiple events when all devices directly below the gate must fail in order to have a failure above the gate.

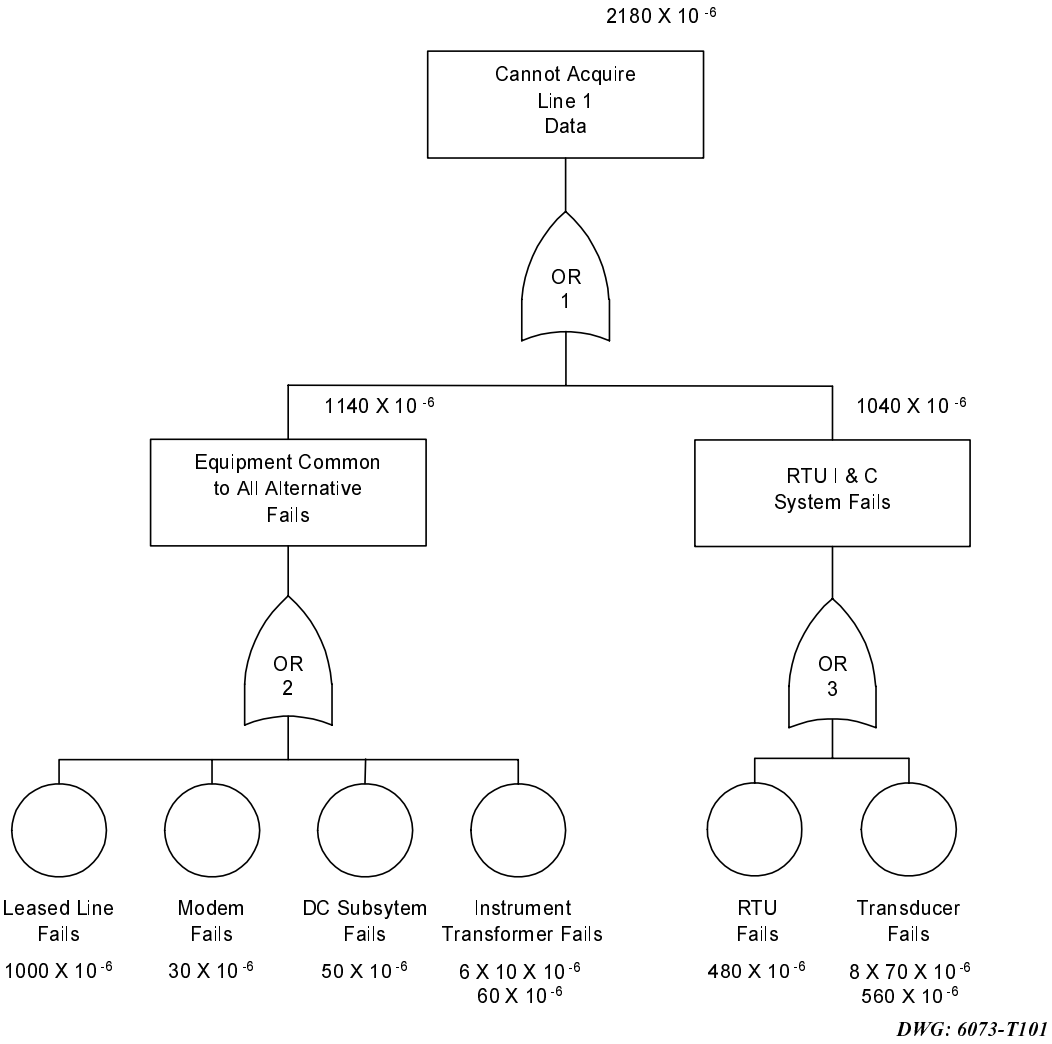

Figure 2: Fault Tree for RTU System in Six-Line Substation

Fault Tree Analysis

After entering event data, analysis of the fault tree shown in Figure 2 is straightforward using a single simplifying assumption known as the Rare Event Approximation. It ignores the possibility that two or more rare events can occur simultaneously. For two events, each of which occurs with probability less than 0.1, the rare event approximation produces less than 5% error. When the events in question are failures, the rare event approximation is always conservative; the approximated probability of failure is always greater than the actual probability of failure [1].

Employing the rare event approximation, calculate the unavailability associated with each event expressed with an OR gate as the sum of the unavailability for each input to the OR gate. For example, the unavailability associated with Gate OR 2 is the sum of the unavailability of the four inputs to that OR gate. The fault tree of Figure 2 contains only basic events and OR gates. Therefore the unavailability associated with the Top Event is simply the sum of all of the basic events or $2180 \cdot 10^{-6}$.

COMPARISON OF I&C ALTERNATIVES FOR AN EXAMPLE ELECTRICAL SUBSTATION

Fault trees in this section contrast the unavailability of I&C examples for control and data acquisition for one line of a six-line substation. The unavailabilities of the compared systems are summarized in Table 2.

Fault Tree for an RTU-Based I&C System

Consider a top event that includes obtaining analog data and sensing and operating Breaker 1. The failure of the breaker contributes to the new top event. These changes are shown in the fault tree of Figure 3. The triangle on the left of the drawing with a line from the side identifies a fragment of the fault tree which can be used on other fault trees by reference. In subsequent fault trees in this section we reference this same "Equipment Common to All Alternatives Fails" from the fault tree of Figure 3. I used a leased line in the examples because most installed SCADA systems in the United States use leased lines.

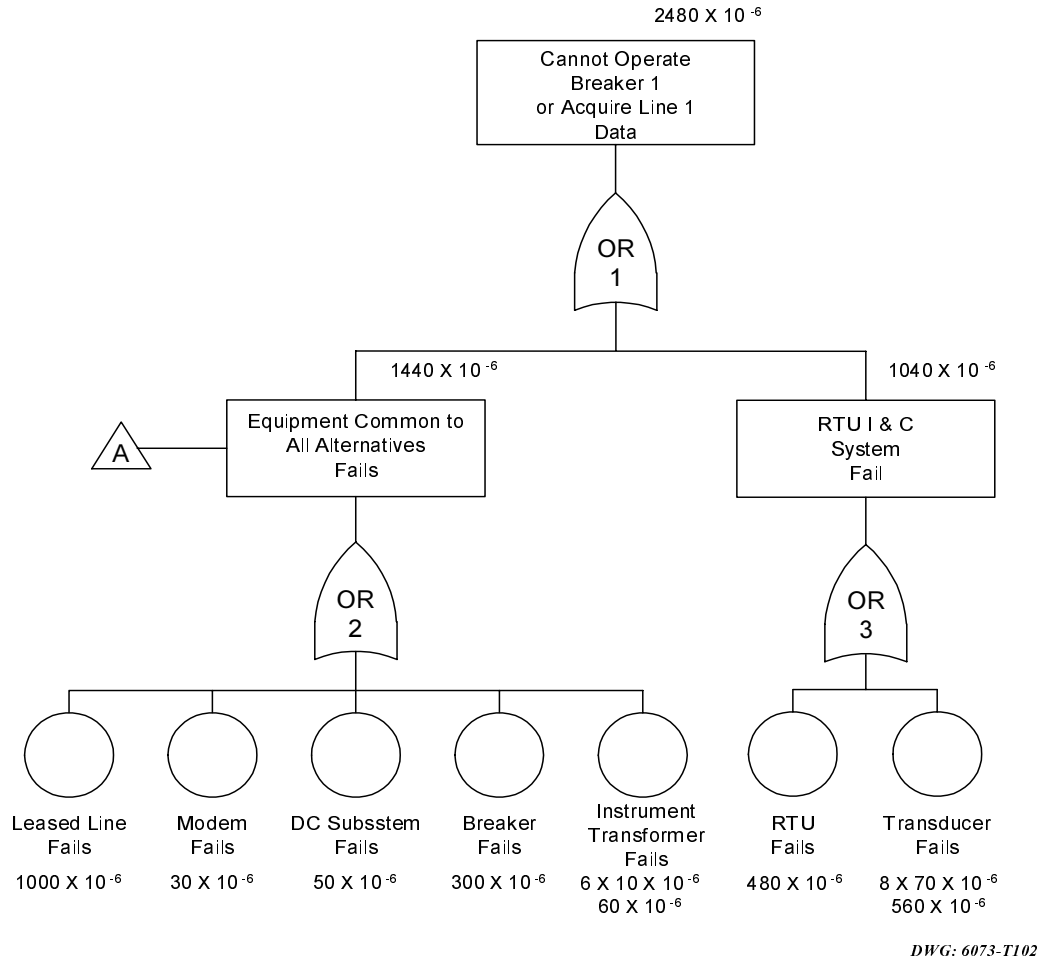

Figure 3: Fault Tree for RTU-Based I&C System in Six-Line Substation

Fault Tree for a Relay and Communications Processor Star I&C System

The fault tree in Figure 4 includes a relay for each line and a communications processor to link them together and communicate with the master. See the Appendix for similar fault trees for a personal computer and industrial computer as the hubs of a star network connected to relays.

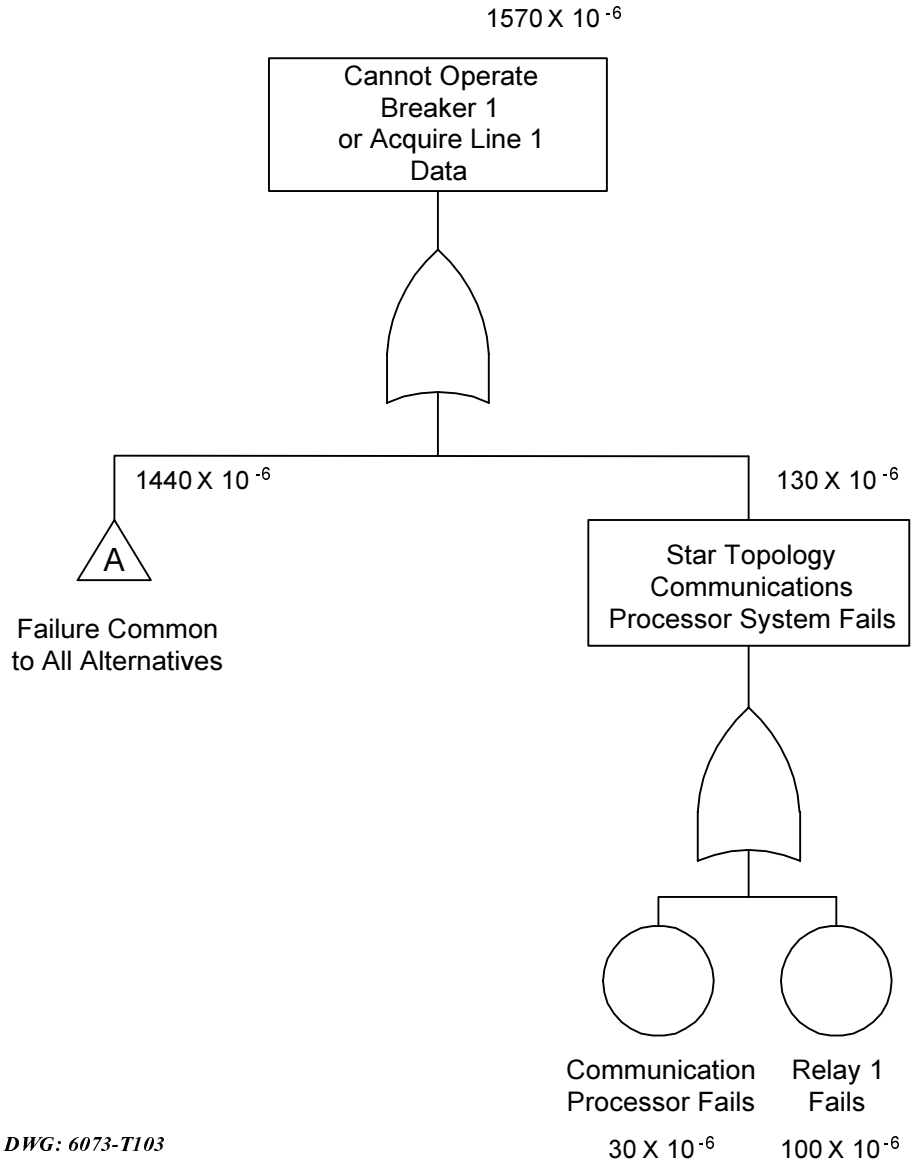

Figure 4: Fault Tree for Relay and Communications Processor Star I&C System in a Six-Line Substation

Fault Tree for a PC Connected to A Multidrop Relay Network

The fault tree in Figure 5 is for a system with a personal computer connected to relays through a multidrop network rather than the star configuration used in all the previous examples. In a multidrop network a device can fail in a mode which prevents communications on the network. This type of failure is a small subset of the total failure modes of the networked device. I used an MTBF of 500 years for each of the other relays to fail with this impact. Similar fault trees using an industrial PC and a Programmable Logic Controller are in the Appendix.

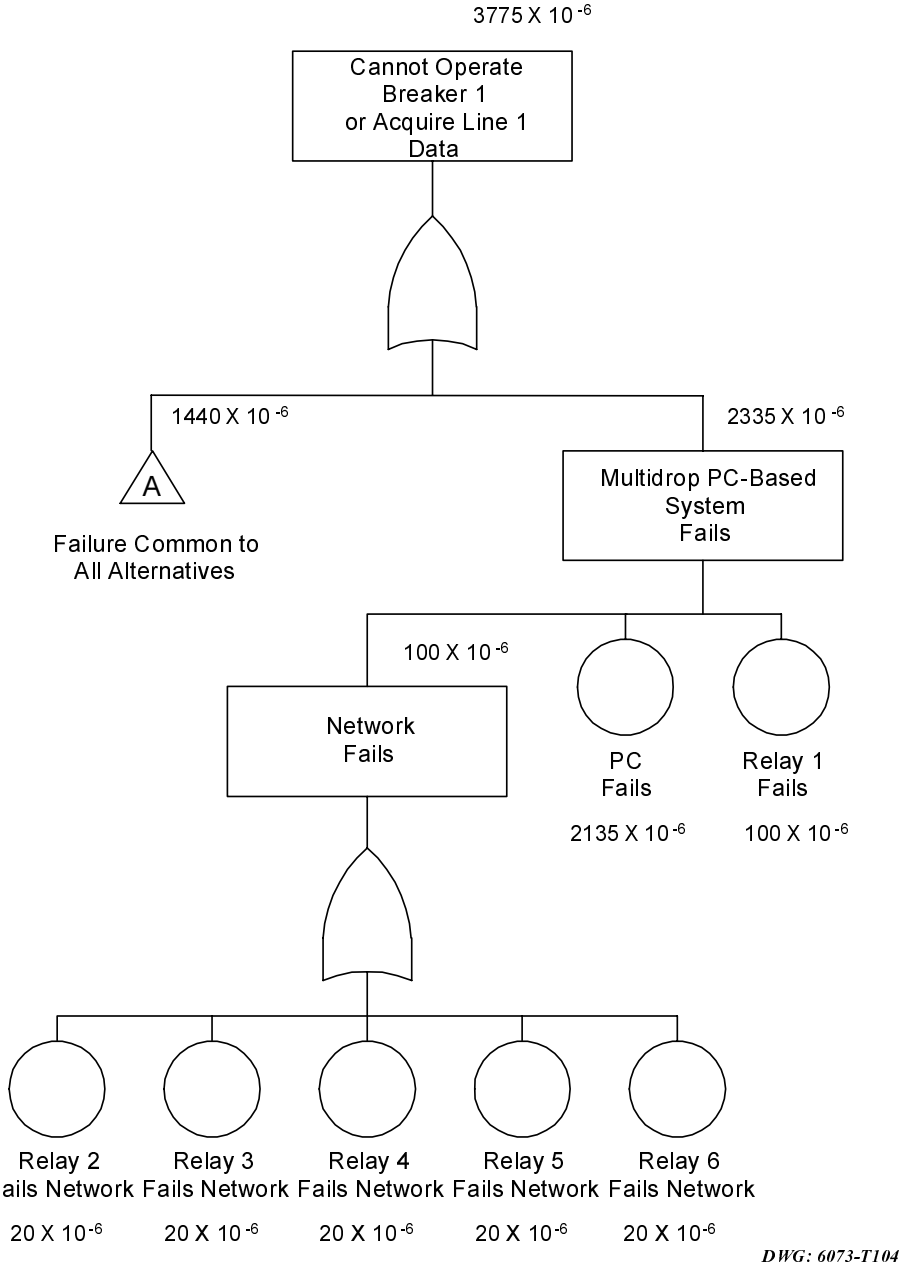

Figure 5: Fault Tree for a PC Multidrop Relay Network in a Six-Line Substation

Summary of I&C System for Example Six-Line Substation

From Table 2 observe that for these examples the most reliable I&C system has eighteen times better unavailability than the least reliable system.

Table 2: Approximate Unavailabilities of Six-Line Substation Systems for Top Event *Cannot Sense or Operate Line 1*

System	I&C Unavailability	Total Unavailability
RTU-based	1040×10^{-6}	2480×10^{-6}
Communications processor star to relays	130×10^{-6}	1570×10^{-6}
PC star to relays	2235×10^{-6}	3675×10^{-6}
Industrial computer star to relays	485×10^{-6}	1925×10^{-6}
PC multidrop to relays	2335×10^{-6}	3775×10^{-6}
Industrial PC multidrop to relays	585×10^{-6}	2025×10^{-6}
PLC multidrop to relays	520×10^{-6}	1960×10^{-6}

COMPARISON OF OVERALL SYSTEM UNAVAILABILITY FOR I&C ALTERNATIVES

It is important to choose a top event which provides useful information. You can also evaluate the I&C system alternatives from the previous example using the top event of "Any Analog Data Unavailable or Any Breaker is Inoperable." This will yield unavailability of the whole substation. The fault tree in Figure 6 for a communications processor star includes the additional substation apparatus and I&C system for the six-line substation of the previous example. All six breakers are included in the total, with six sets of instrument transformers, and six relays.

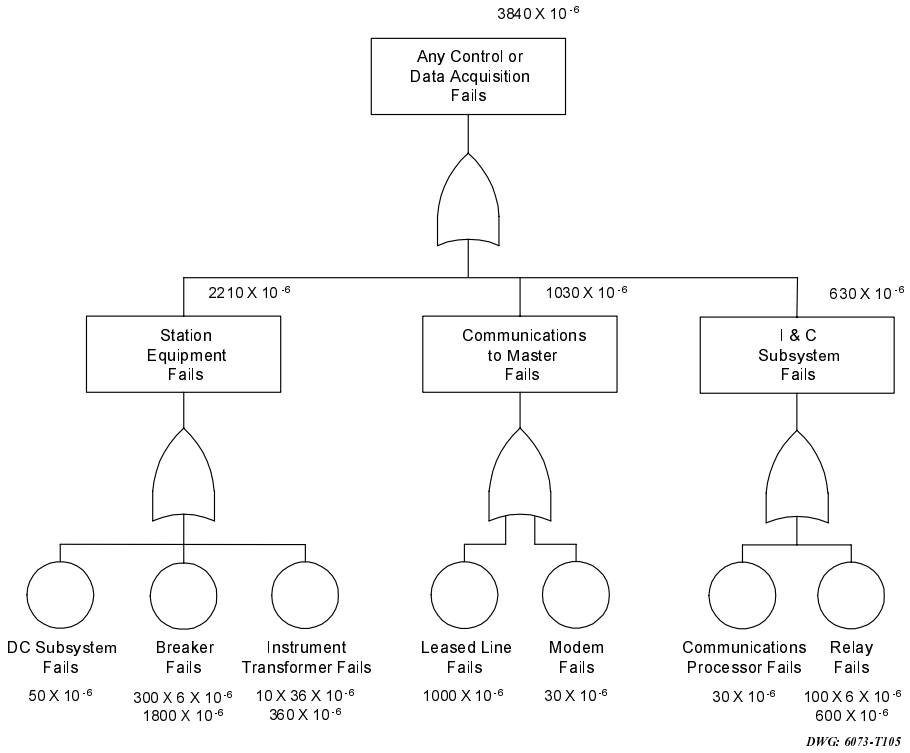

Figure 6: Fault Tree for Any Failure of Relay and Communications Processor Star I&C System in a Six-Line Substation

Figure 7 is a fault tree for a PLC-based multidrop network with six relays. Choosing this top event will yield the unavailability of the system, defined as **any** device failure. In contrast to the first example, it defines the system as unavailable if any part of it is failed. In other words, if any device fails, the system is considered unavailable, even though many portions of the system could be functioning. This analysis does not require a separate event for failure due to the network failure of a relay because every relay failure causes the top event. Since no credit is given for partial availability with this top event, the difference in unavailabilities of star and multidrop systems is not as large as in the previous examples. The other alternatives have fault trees similar to Figures 6 and 7; the fault trees are omitted for brevity but are summarized in Table 3.

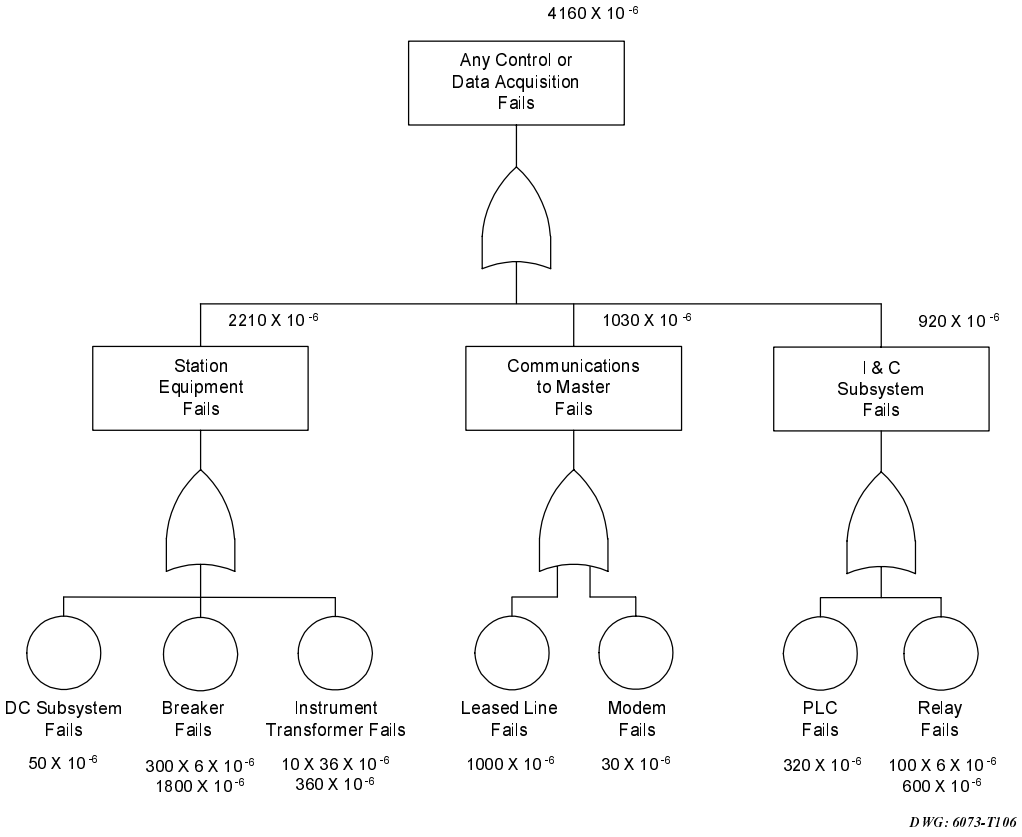

Figure 7: Fault Tree for Any Failure of PLC Connected to a Multidrop Network in a Six-Line Substation

From Table 3 observe that for these examples the most reliable I&C system has four times better unavailability than the least reliable system.

Table 3: Approximate Unavailabilities of Six-Line Substation Systems Top Event *Any Control or Data Acquisition Fails*

System	I&C Unavailability	Total Unavailability
Communications processor star to relays	630×10^{-6}	3840×10^{-6}
PC star to relays	2735×10^{-6}	5975×10^{-6}
Industrial computer star to relays	985×10^{-6}	4225×10^{-6}
PC multidrop to relays	2735×10^{-6}	5975×10^{-6}
Industrial PC multidrop to relays	985×10^{-6}	4225×10^{-6}
PLC multidrop to relays	920×10^{-6}	4160×10^{-6}

RTU AND COMMUNICATIONS PROCESSOR IN PARALLEL

Until recently electric utility engineers have generally viewed SCADA and protection functions as distinct and unrelated to one another. As a consequence many substations have an RTU-based SCADA system and separate protective relays. If the relays are microprocessor-based with communications capability, adding a communications processor creates a backup system to the RTU for line data and breaker control. If a backup communications channel is provided that does not share common failure causes with the primary channel, then the channel and modem can be included in each subsystem to further improve reliability. Recall that you use an AND gate to combine multiple events when all devices directly below the gate must fail in order to have a failure directly above the gate. Figure 8 shows the fault tree for the primary RTU system of Figure 3, combined with the star topology of Figure 4. The overall system has an unavailability of 410×10^{-6}. Compare this to the availabilities of 2480×10^{-6} for the system of Figure 3 and 1570×10^{-6} for Figure 4.

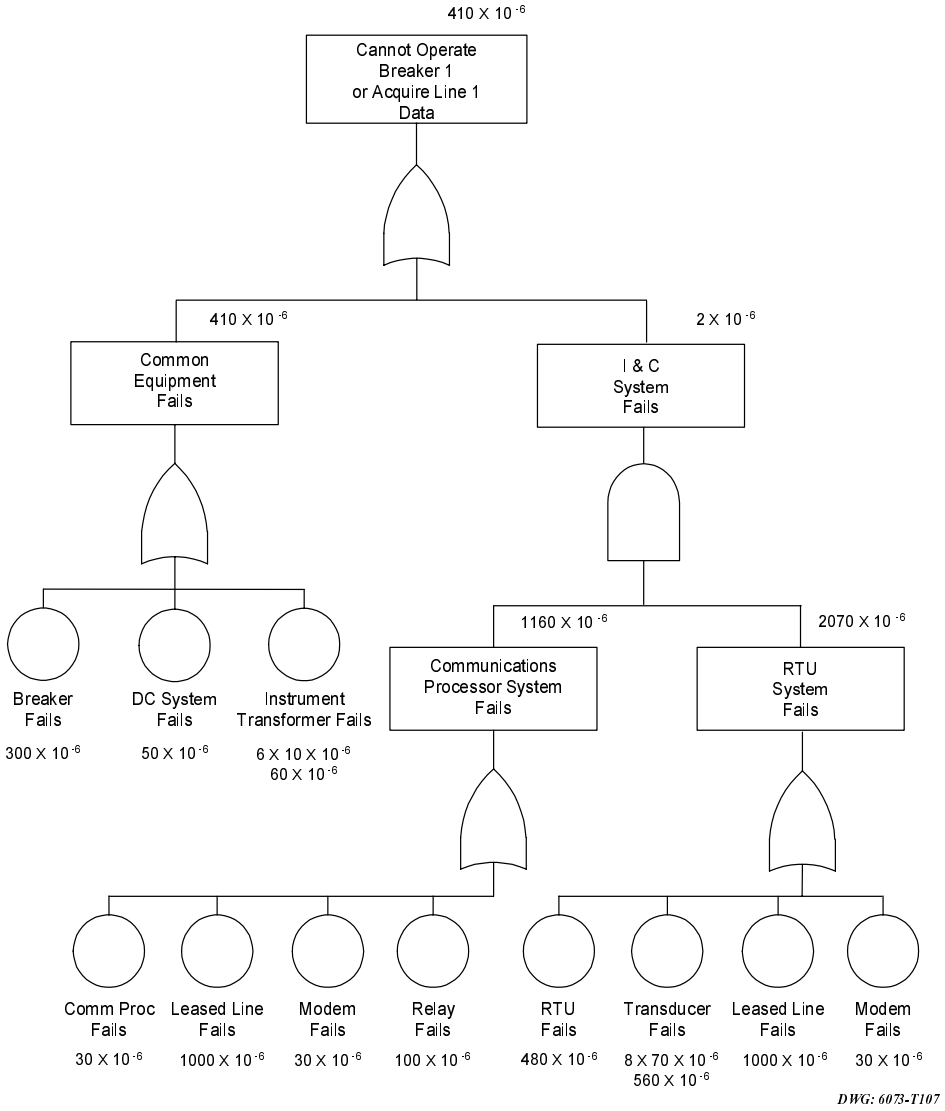

Figure 8: Fault Tree for RTU and Communications Processor/Relay System in a Six-Line Substation

DUAL I&C SYSTEMS LARGE SUBSTATION EXAMPLE

Providing dual-redundant backup of a device or subsystem will generally improve system reliability. As you construct the fault tree for dual systems be careful that the inputs to an AND gate do not share common failure events. The examples in this section for a large substation are based on I&C alternatives that a large utility considered for a substation with 54 lines with microprocessor-based line protection relays. One alternative considered used communications processors in a star topology, Figure 9.

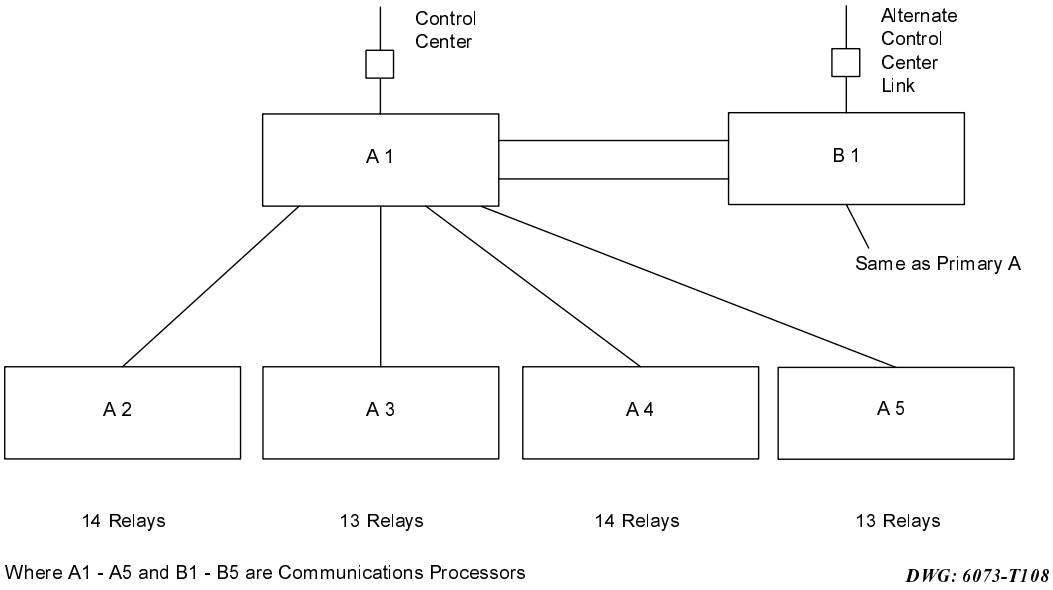

Figure 9: Block Diagram of Communications Processor I&C System for 54-Line Substation

Due to the large number of relays, a top-tier communications processor (A1) was used to communicate with four communications processors (A2, A3, A4, and A5). These in turn communicated with 54 relays. The entire system was replicated for the backup system. Figure 10 is the fault tree for unavailability of data or control for a single line or breaker. Figure 11 is the fault tree for unavailability of any data item or any control action.

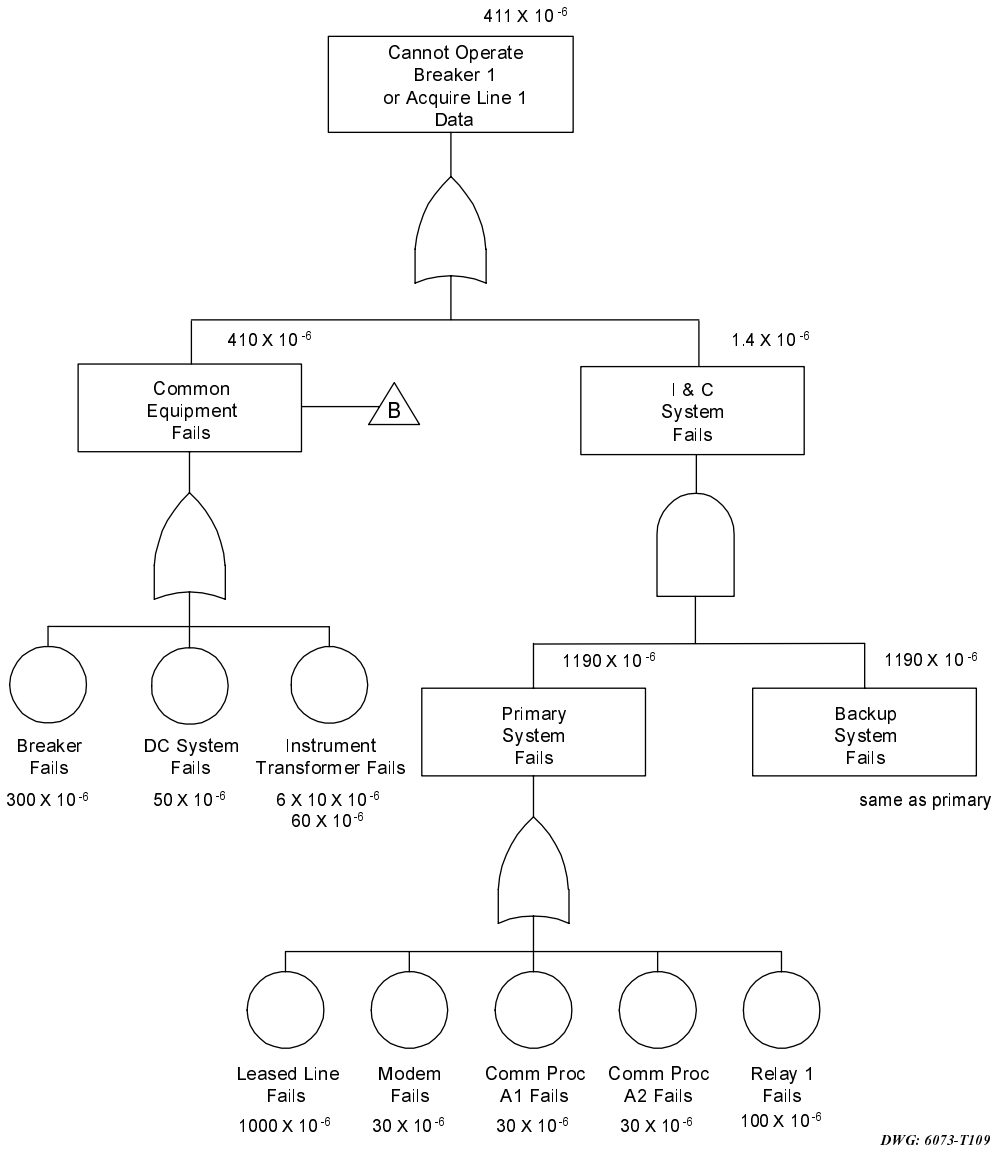

Figure 10: Fault Tree for Communications Processor I&C System for 54-Line Substation

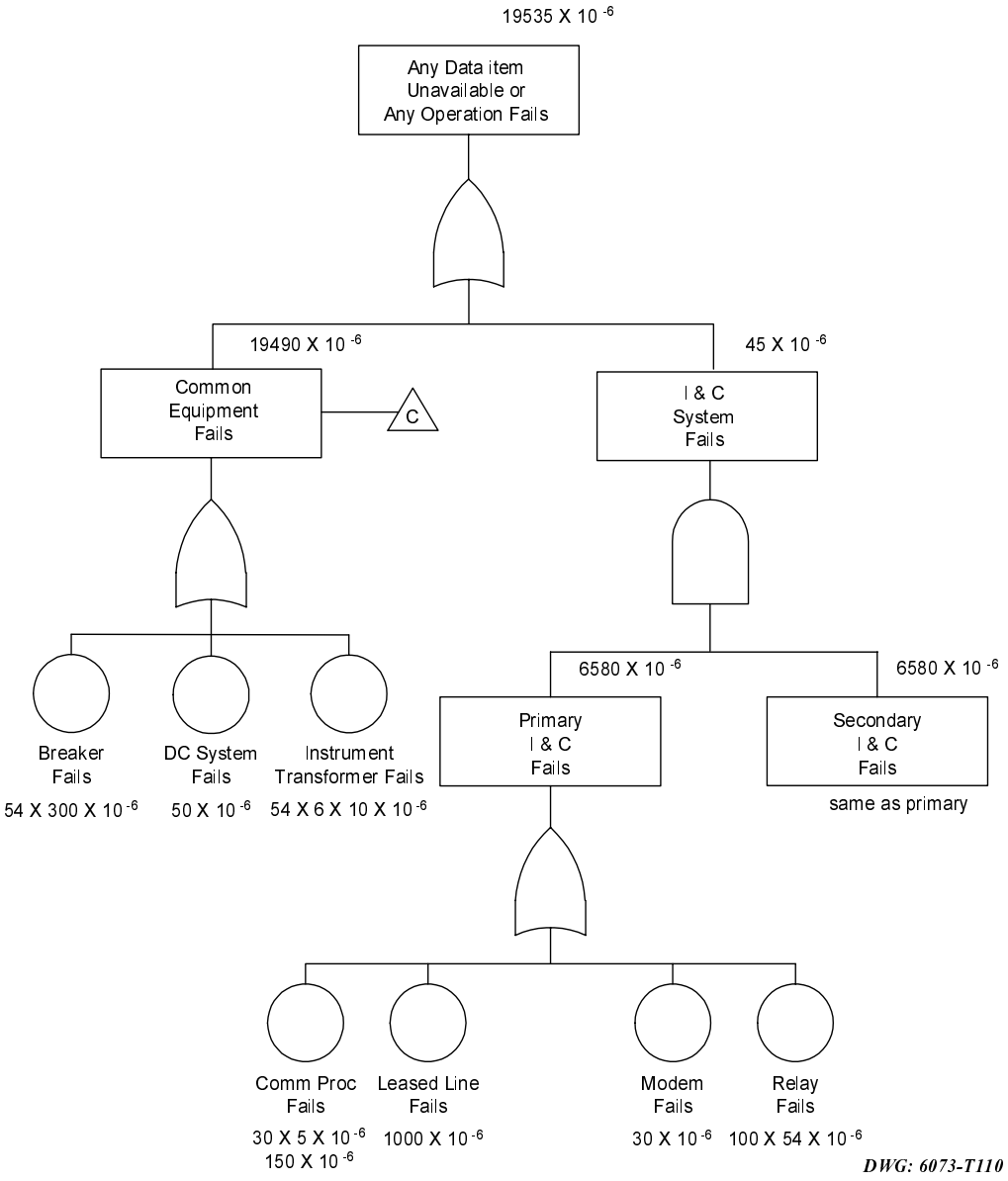

Figure 11: Fault Tree for Any Failure of Communications Processor I&C System for 54-Line Substation

The proposed alternative was a personal-computer-based system as shown in Figure 12, with two communications lines and a multidrop network connection to the relays.

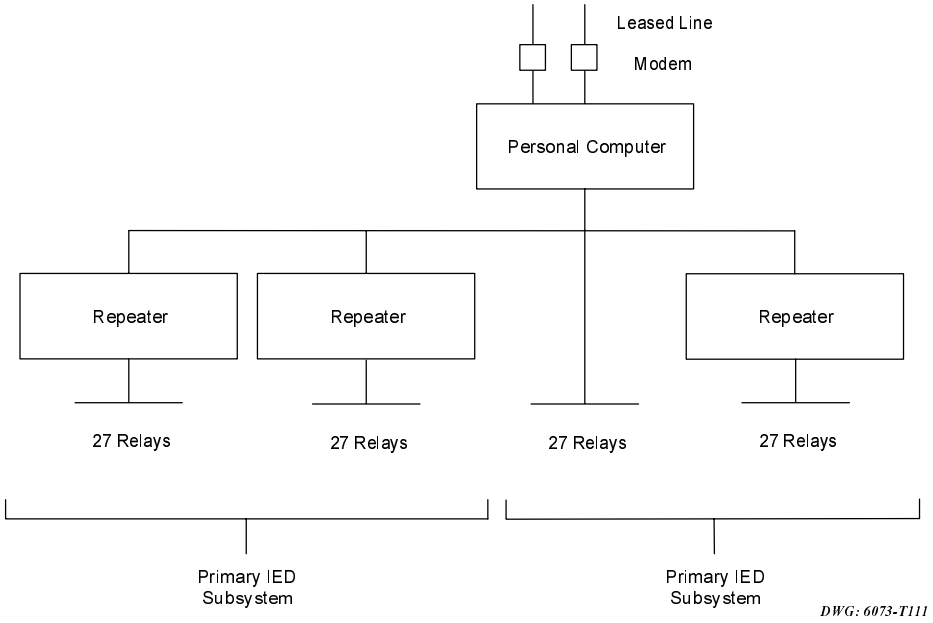

Figure 12: Block Diagram for PC Multidrop I&C System for 54-Line Substation

Because the network involved had a physical connection limit of 31 devices, three repeaters were required to communicate with the 108 relays in the primary and backup protection schemes. Figure 13 is the fault tree for unavailability of a single line or breaker data. Figure 14 is the fault tree for unavailability of any data item or any control action.

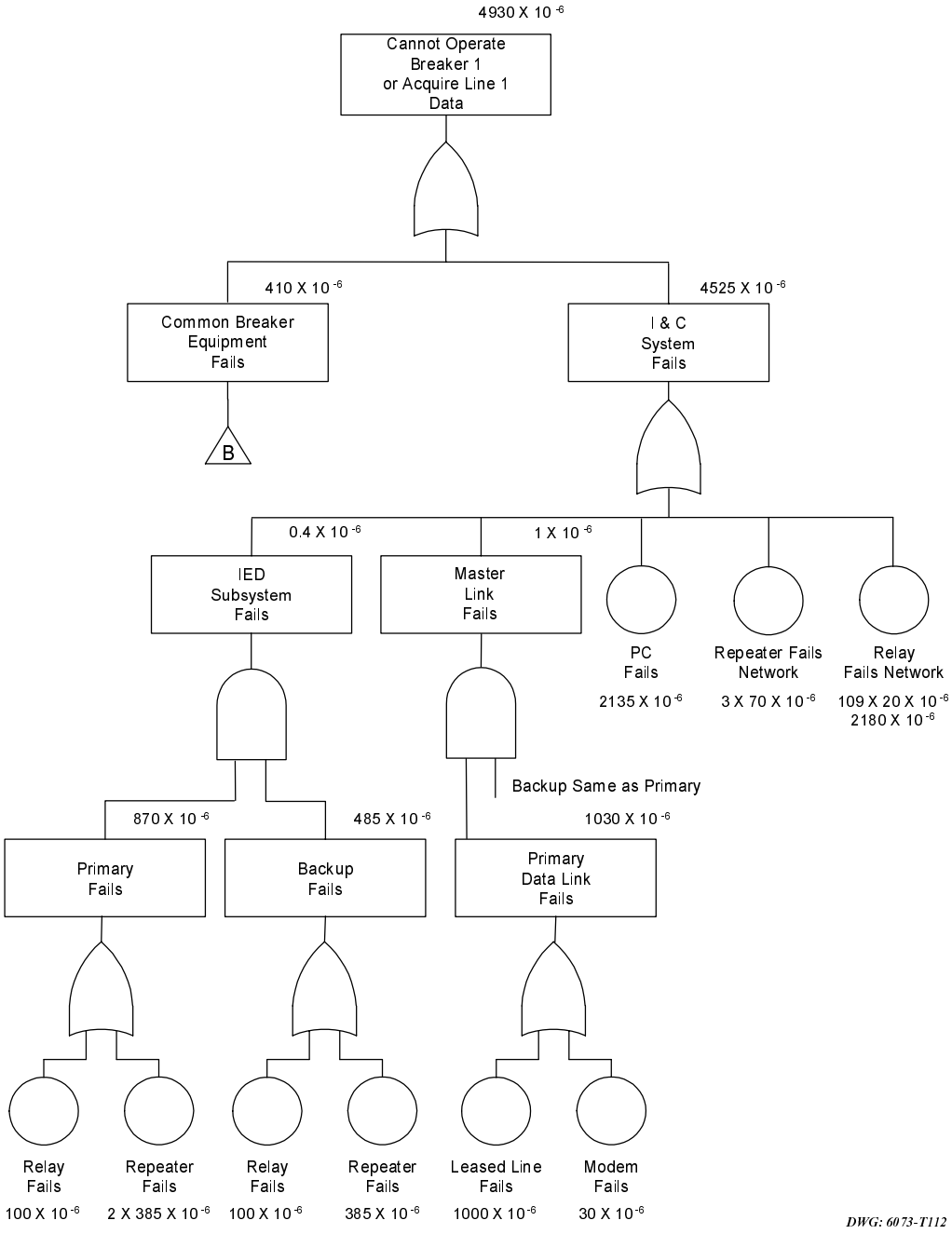

Figure 13: Fault Tree for PC Multidrop I&C System for 54-Line Substation

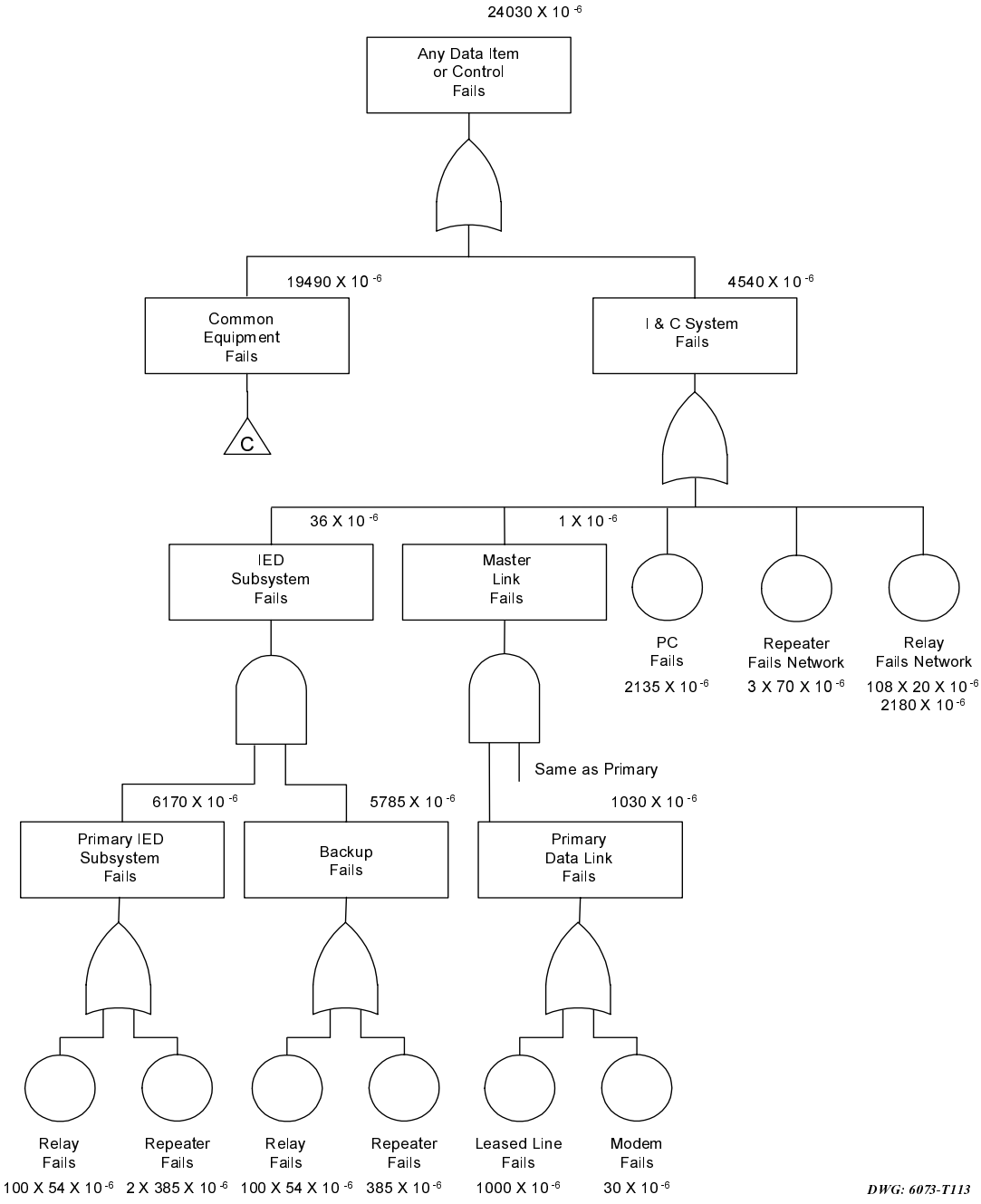

Figure 14: Fault Tree for Any Failure of PC Multidrop I&C System for 54-Line Substation

These alternatives were first analyzed with regard to equipment cost, development cost, and performance. The redundancy of the communications processors of Figure 9 was initially due to the number of relays and the number of ports on each processor. Option 1 was initially selected on the basis of cost and performance. A subsequent analysis revealed that the selected system was significantly more reliable, as shown by the Figures 10, 11, 13, 14, and Table 4.

Table 4: Unavailabilities of 54-Line Substation System Examples

System and Top Event	I&C Unavailability	Total Unavailability
Unavailability of a Single Line or Breaker Data or Control:		
Multiple communications processor star to relays	1×10^{-6}	410×10^{-6}
PC multidrop to relays	4525×10^{-6}	4930×10^{-6}
Unavailability of Any Line or Breaker Data or Control:		
Multiple communications processor star to relays	45×10^{-6}	$19{,}535 \times 10^{-6}$
PC multidrop to relays	4540×10^{-6}	$24{,}030 \times 10^{-6}$

SUMMARY

The purpose of this paper is to introduce fault tree analysis as a tool for substation I&C designers to assess the reliability of alternative systems and to identify changes that will yield significant improvements in reliability. The examples show that relatively small fault trees are simple to construct and analyze, and reveal useful information about the reliability of substation equipment and control systems.

I omitted some root events from the examples for clarity because their affects were numerically insignificant.

I did not include the unavailability of software in the PC-based systems because I did not locate sufficient nor consistent data to approximate the unavailability of operating systems and application programs**.** Further work is warranted to identify and quantify the inputs to predict the reliability of software.

Fault trees are used for more thorough and complex analysis than the examples presented here. There are additional techniques, symbols, and rules to support such analyses. There is a large body of reference work from the nuclear and reliability engineering disciplines which demonstrate other aspects of fault tree construction and analysis. I recommend Reference 2 for those interested in learning more about fault trees. Other tools are suitable for estimating the unavailability, including the Markov models used in Reference 3.

In conclusion:

1. Designers can use fault tree analysis to easily compare the reliability of alternatives for substation instrumentation and control.

2. Determine the unavailabilities for devices that can impact the Top Event to identify actions to improve overall system availability, and assess the relative significance of improvements in the availability of a given component or subsystem. Then, use fault trees to help you predict the unavailability of the resulting system.

3. Carefully choose the Top Event to provide a meaningful comparison of alternatives. If loss of communications with one device has different consequences than loss of communications with all devices, then you should model both cases to understand the availability of both.

4. Providing a redundant subsystem without shared failure mechanisms can dramatically improve the availability of the combined subsystem.

5. Many substations contain numerical protective relays which provide an opportunity to improve the reliability of the SCADA system.

APPENDIX

These are the additional fault trees referenced in the text.

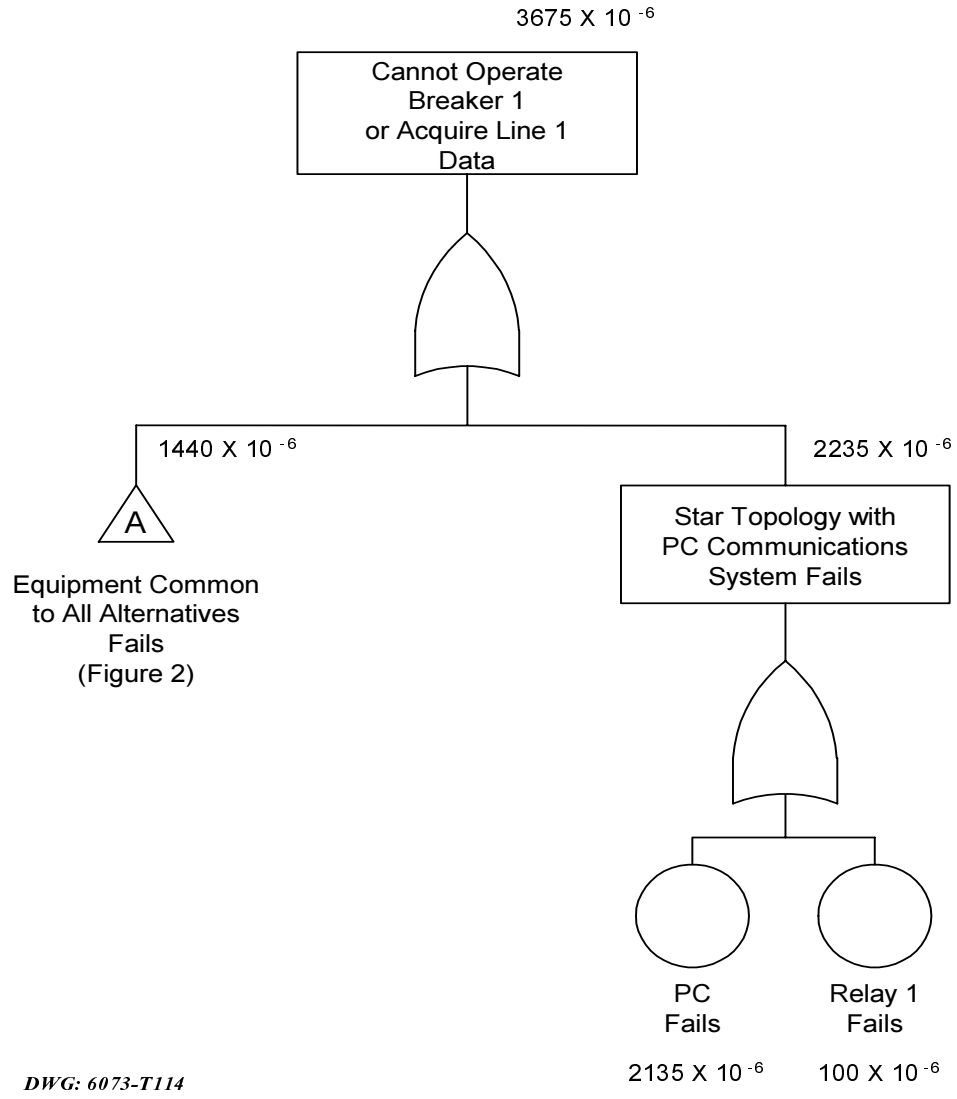

Figure 15: Fault Tree for Relay and PC Star I&C System in a Six-Line Substation

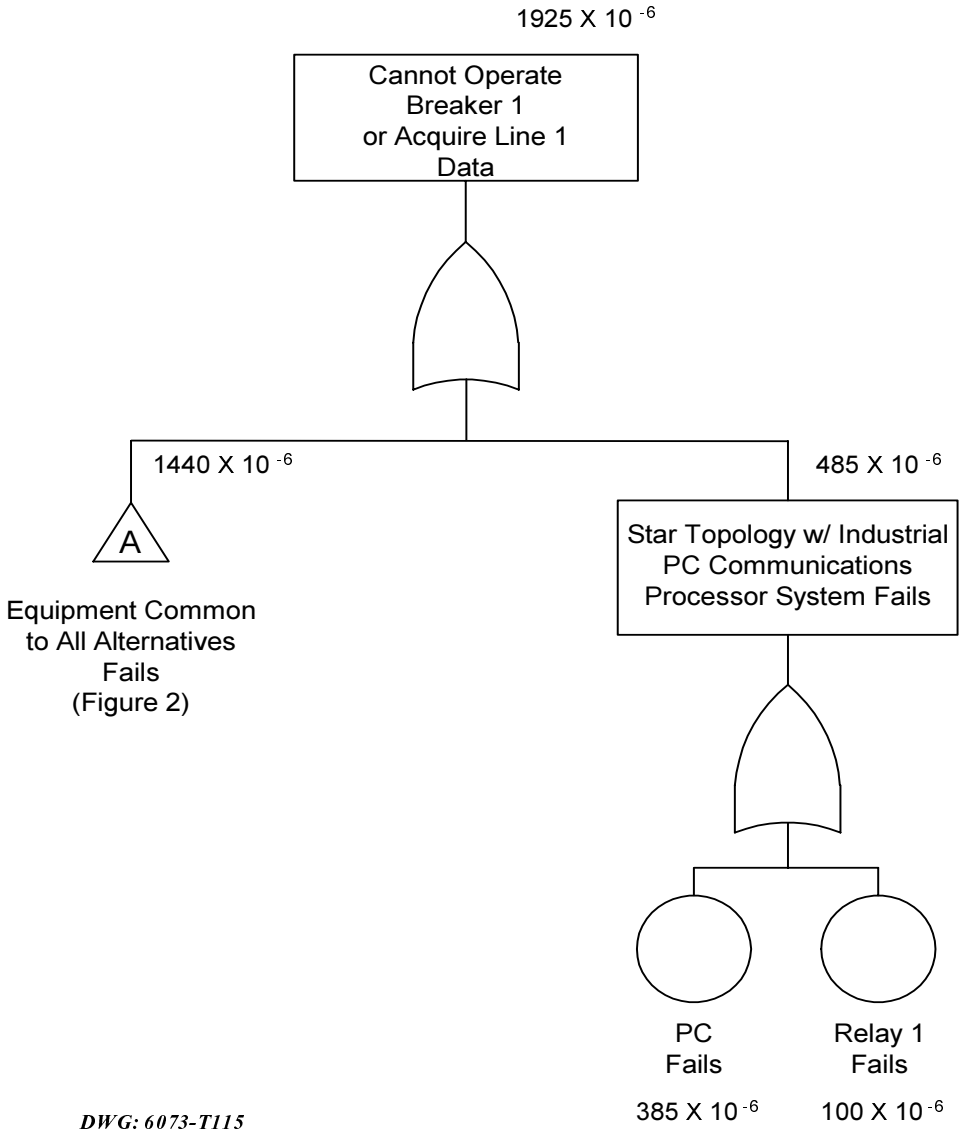

Figure 16: Fault Tree for Relay and Industrial PC Star I&C System in a Six-Line Substation

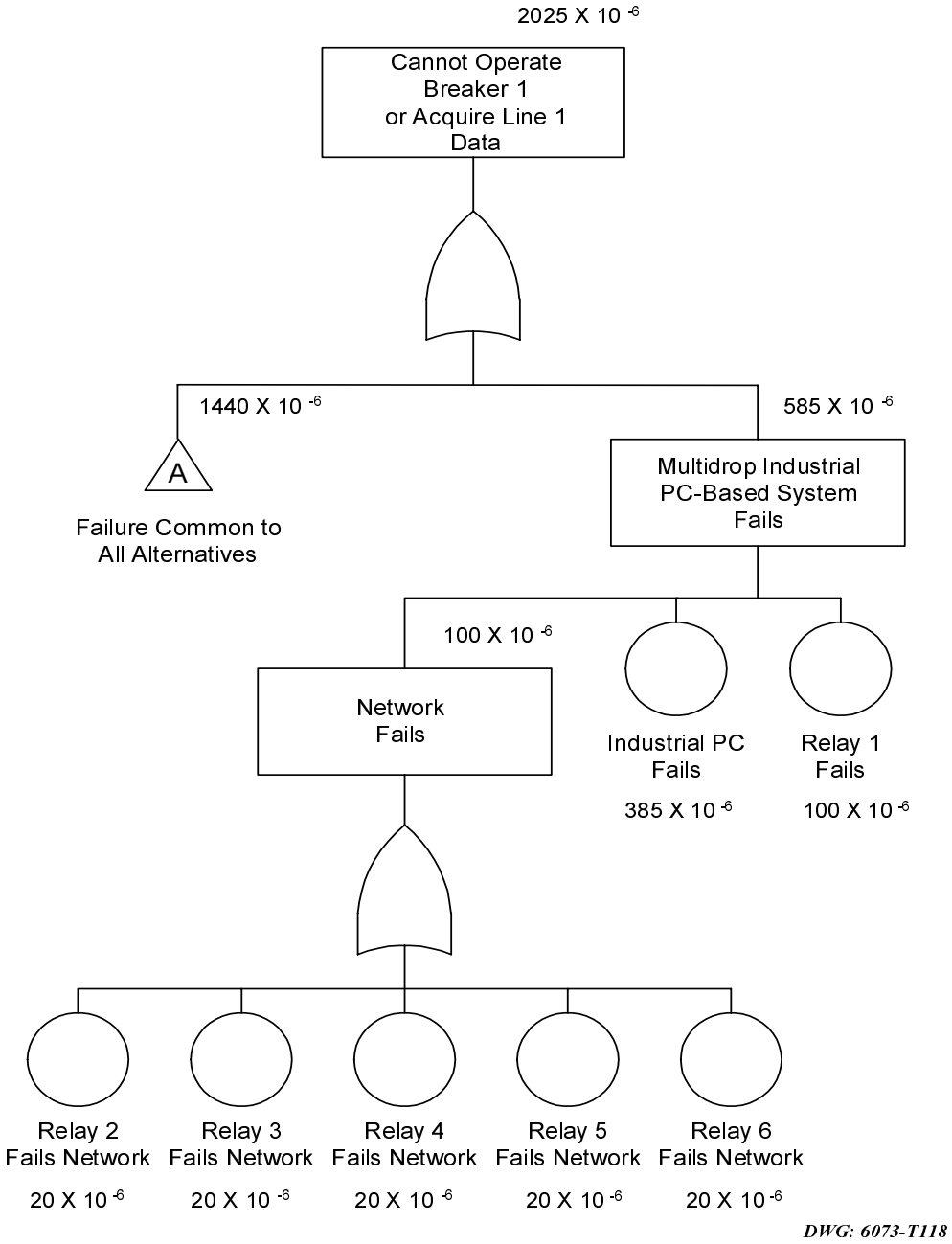

Figure 17: Fault Tree for Industrial PC Multidrop Network in a Six-Line Substation

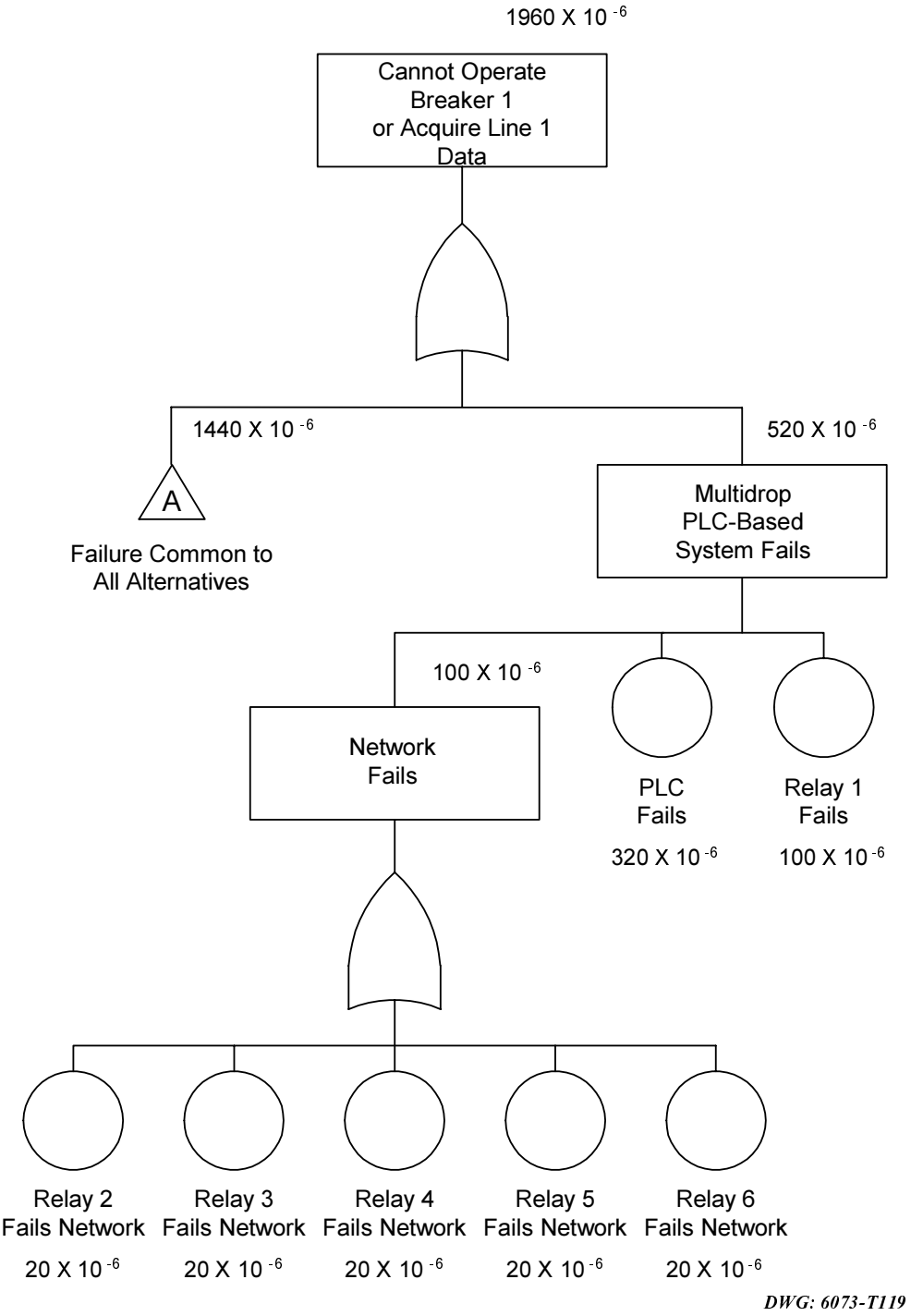

Figure 18: Fault Tree for PLC Multidrop Network in a Six-Line Substation

REFERENCES

[1] P. M. Anderson, B. Fleming, T. J. Lee, E. O. Schweitzer, III, "Reliability Analysis of Transmission Protection Using Fault Tree Methods," Proceedings of the 24th Annual Western Protective Relay Conference, Spokane, Washington, October 21 - 23, 1997.

[2] N. H. Roberts, W. E. Vesely, D. F. Haasl, and F. F. Goldberg, "Fault Tree Handbook" NUREG-0492m U.S. Nuclear Regulatory Commission, Washington, DC, 1981.

[3] John J. Kumm, Edmund O. Schweitzer, III, and Daqing Hou, "Assessing the Effectiveness of Self-Tests and Other Monitoring Means in Protective Relays," Proceedings of the 21st Annual Western Protective Relay Conference, Spokane, WA, October 18 - 20, 1994.

[4] J. Palomar, R. Wyman, "The Programmable Logic Controller and Its Application in Nuclear Reactor Systems, Fission Energy and Systems Safety Program, Lawrence Livermore National Laboratory, June 30, 1993.

[5] C. M. Mitchell, K. Williams, "Failure Experience of Programmable Logic Controllers Used in Emergency Shutdown Systems," Reliability Engineering & System Safety, Vol. 39 No. 3, 1993, pp 329-31.

[6] H. Martini Paula, "Failure Rates for Programmable Logic Controllers," Reliability Engineering & System Safety, Vol. 39 No. 3, 1993, pp 325-8.

BIOGRAPHY

Gary W. Scheer received his BSEE from Montana State University in 1977. He worked for the Montana Power Company and Tetragenics Company before joining Schweitzer Engineering Laboratories, Inc. in 1990 as a development engineer. He was Manager and Vice President of Research and Development. He now serves as Vice President of Automation and Engineering Services. He holds one patent and has another pending. He is a registered Professional Engineer and is a member of the IEEE and the ISA.