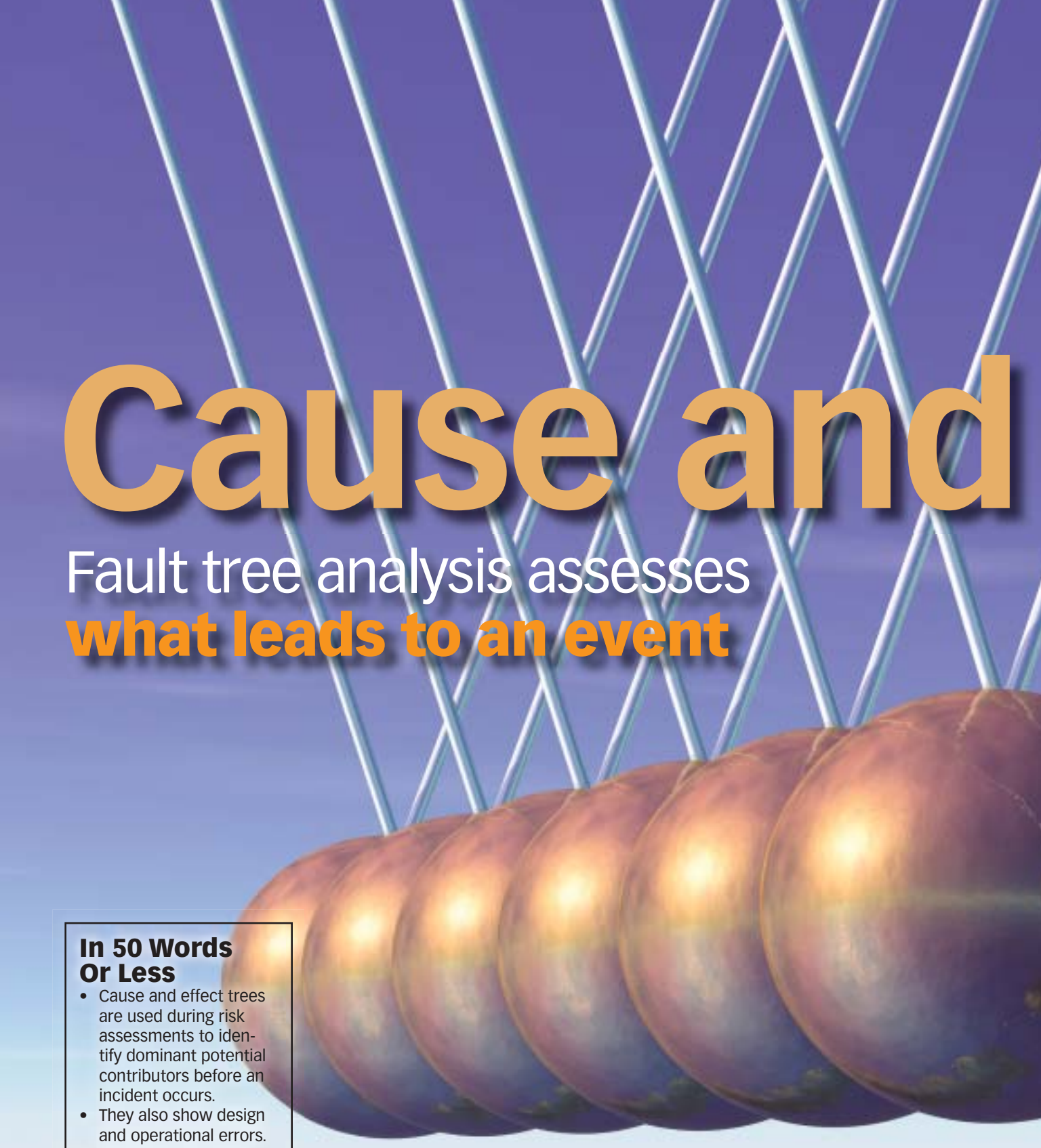
Cause and

Fault tree analysis assesses **what leads to an event**

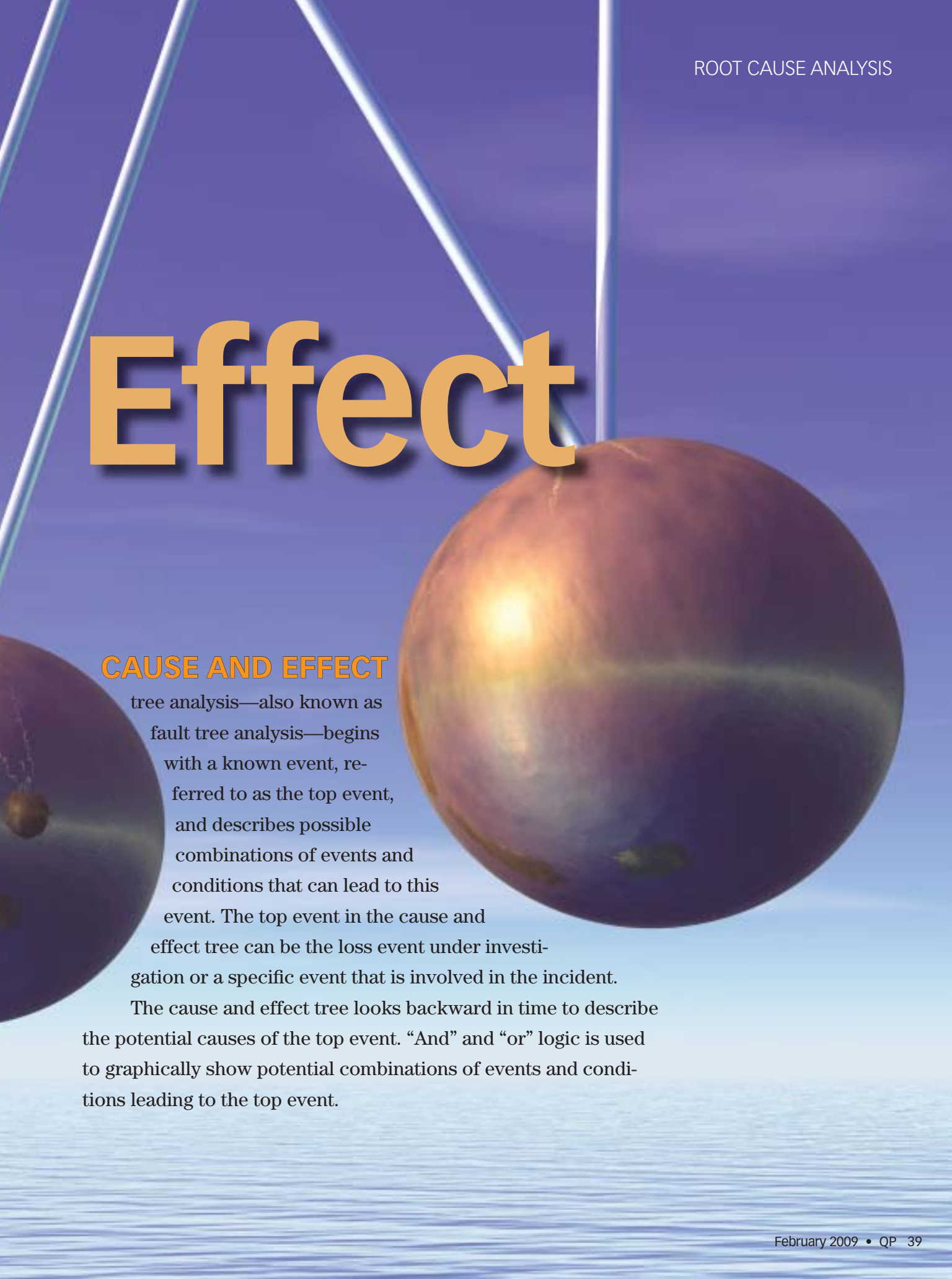


In 50 Words Or Less

- Cause and effect trees are used during risk assessments to identify dominant potential contributors before an incident occurs.
- They also show design and operational errors.
- "And" and "or" gates connect the sets of causes and effects, and a single item can be both a cause and effect.

by James J. Rooney, Lee N. Vanden Heuvel, Donald K. Lorenzo and Laura O. Jackson

Effect



CAUSE AND EFFECT tree analysis—also known as fault tree analysis—begins with a known event, referred to as the top event, and describes possible combinations of events and conditions that can lead to this event. The top event in the cause and effect tree can be the loss event under investigation or a specific event that is involved in the incident.

The cause and effect tree looks backward in time to describe the potential causes of the top event. "And" and "or" logic is used to graphically show potential combinations of events and conditions leading to the top event.

Cause and effect trees were first developed by Bell Laboratories in the 1960s, and the technique remains relevant today. Quality professionals should have a firm grasp of this important problem solving method.

The technique is commonly used during risk assessments to identify dominant potential contributors before an incident occurs. For incident investigation applications, however, the smallest possible tree is developed. As soon as a branch is shown not to be credible (proven false), development of that branch is stopped.

Most proactive and reactive analysis techniques identify only failures caused by a single event. One significant advantage of the cause and effect tree technique is that it can help identify multiple-event failures, which require more than one event for a failure to occur.

For example, for fire to form, three conditions must exist simultaneously: fuel, oxygen and an ignition source. Most incidents involve multiple-event failures. The ability to model multiple-event failures is therefore an essential element for any incident modeling method.

A cause and effect tree can also show design and operational errors. In some cases, equipment performs to its capabilities, but these capabilities are insufficient for the task. For example, a generator failed when it was overloaded, or a pump was designed to deliver 100 gallons per minute (gpm), but 150 gpm was required.

Basic structure

Cause and effect trees are constructed with sets of causes and effects that are connected by gates. Figures 1 and 2 show the basic elements of a cause and effect tree.

There are two types of gates: "and" gates and "or" gates. When referring to them generically, they are simply called gates. The effect is above the gate, and the causes are below. Note that a single item on the tree can be a cause and an effect, depending on which gate you are examining. For example, in Figure 3, Item 4 is a cause of Item 1. Item 4 is the effect of Cause 5 or Cause 6. For any gate on the tree, the event above the gate is the effect, and the events below the gate are the causes.

Three examples

Example 1—spill from a tank: Figure 4 shows a portion of a cause and effect tree for a spill from a tank. In this case, three possible causes of the spill were identified by the investigator:

1. Misdirected flow.
2. Excessive flow.
3. Failed tank or piping.

Each of these causes is sufficient to cause the spill from the tank, so an "or" gate is used. Next, each of these three items is examined to determine its causes.

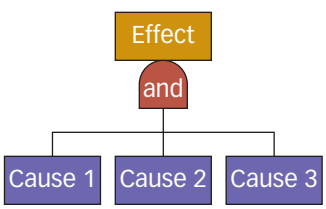
For the misdirected flow event, two events must be present at the same time: Valve 1 must be closed, and Valve 2 must be open. Closing Valve 1 is not enough to cause the misdirected flow. If Valve 2 is also closed, the flow will not go through Valve 1 or Valve 2. Because the line with Valve 1 is so much larger than the line with Valve 2, Valve 1 must be closed to force flow through Valve 2. Therefore, both conditions must be present for the misdirected flow to occur, so an "and" gate is used.

To cause the other two events, excessive flow and failed tank or piping, two possibilities are identified for each. Either item is sufficient to cause the event above it, so "or" gates are used. In this example, there are five combinations of events that can cause the top event:

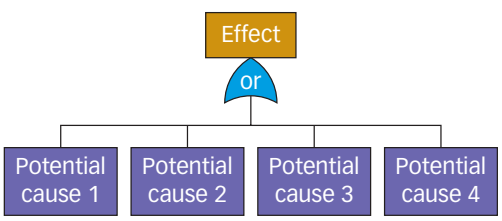
1. Valve 1 closed and Valve 2 open.
2. Normal flow not stopped in time.
3. Tank full before fill started.
4. Failed tank.
5. Failed piping.

In an actual root cause analysis, efforts are made to cut off the branches as soon as possible by collecting

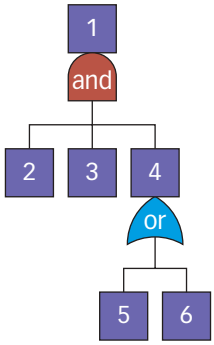
"And" gate structure / FIGURE 1



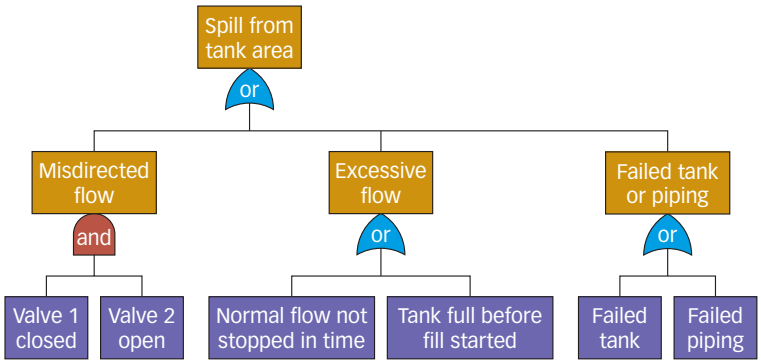
"Or" gate structure / FIGURE 2



Example tree with multiple levels / FIGURE 3



Cause and effect tree for a tank spill / FIGURE 4



data to determine the validity of a branch (whether the branch is true or false). This will be discussed in the next example.

Example 2—lighting failure: Work in a portion of a facility has been halted because the overhead lighting has gone out. The emergency lighting has illuminated, but it is not sufficient to continue normal operations. Quick troubleshooting is needed to determine the source of the problem and restore regular lighting. Figure 5 shows a circuit diagram.

Construction of the cause and effect tree in Figure 6 (p. 42) was based on the assumption the switch and relay were closed before the lighting was lost. The tree starts with very general concepts and works down to specifics. The primary reason for doing this is to minimize effort. In an actual investigation, it is possible that only a small portion of the tree would be needed.

For example, Figure 7 (p. 43) shows just the top of the tree. This is what the tree would look like after the first level was developed. Some effort will be saved if it can be determined which of the branches are correct (true) and which of the branches are incorrect (false). If this can be determined, it may not be necessary to pursue all the branches.

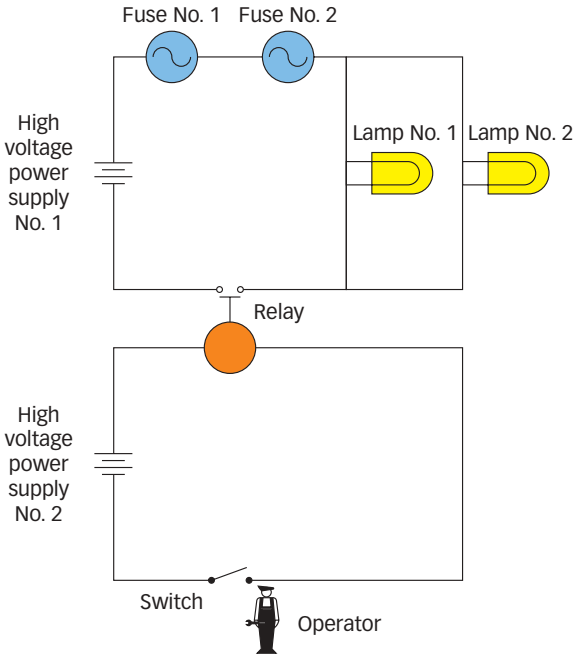
To figure this out, data are needed. A question to ask at this point is, "What data can we collect to determine whether the problem is with the lights, the power or both?" This will help determine what information is needed and how much of the tree to draw.

In case one, an electrician using a multimeter determines there is power to the light sockets. Having this information can save a lot of effort because it is now known that none of the events below Event C are causing a problem with the lights. As a result, no time needs to be spent developing the tree below Event C. Any events below Event C would lead to loss of power to the light socket, and this has just been proven to be false.

To represent this, an X can be put through Event C, and attention can then shift to examining the lights (Event B). Because this is the only other cause identified, replacing the lights should make them operational again.

Case two uses the same test as case one. It is performed by an electrician, but this time the electrician

Circuit diagram / FIGURE 5



says there is no power to the light sockets. Now, more work has to be done to develop the tree below Event C.

While individual components could be tested, it would be better to test on a more global scale, testing many components at the same time. As a result, the next level of the cause and effect tree is developed (see Figure 6) with a general item, "No continuity in high-voltage circuit" (Event D), along with "power supply No. 1 fails off" (event 3).

By testing the continuity in the high-voltage circuit (Event D), a number of components can be checked with a single test. The electrician determines there is no continuity in the circuit. That means the cause and effect tree needs to be developed below Event D.

The next level, with Events E and F, is outlined. First, "relay opened" is investigated. The electrician tests the relay and finds it is closed. An X can now be placed over Event E, and the development of the tree below Event E can be stopped. Finally, it needs to be determined which fuses have failed. Through testing, it is found that both fuses have failed. Events 5 and 6 are circled, and the fuses are replaced. If these are the only failures, the lights will come back on.

For case three, suppose the lights and power to the sockets are tested, and neither is the cause of the failure. To represent this on the tree, an X is put through Events B and C. Now we have a dilemma: The top event is true, but all the causes we have identified (Events B and C) have been eliminated. Now what?

There are two other possible causes of this situation. The first is that there is a cause of the top event that has not been identified. For example, maybe the lights were installed incorrectly or have vibrated loose. Neither of these causes is captured by "both lights have burned out" or "no power to the light sockets."

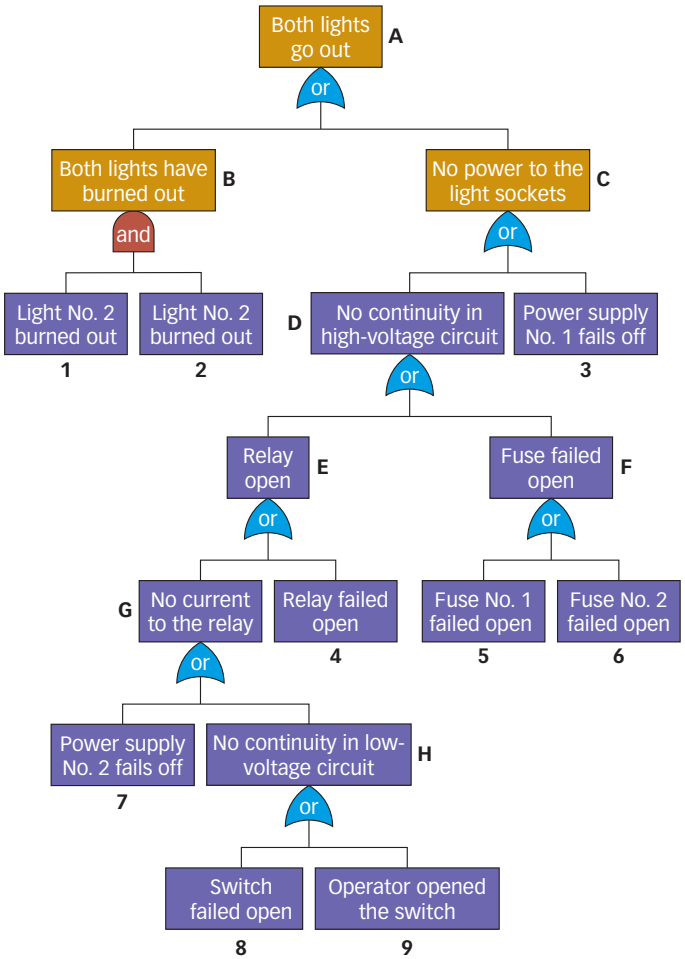
Under Event A, another event needs to be added: "Lights installed incorrectly." Now, the tree reflects the new potential cause that was identified. The second possibility is that one of the tests used to eliminate Events A and B was faulty or incomplete. For example, to test the lights, two new lights were obtained from stores. When these were installed, they did not work. It had already been established there was power to the light sockets, so it was concluded it could not be the bulbs (Events 1 and 2 were crossed out) because they were new. It is unlikely, but both bulbs could be faulty due to damage during shipment, manufacturing errors or damage during storage.

"Light No. 1 burned out" and "light No. 2 burned out" were eliminated (crossed out) as possibilities based on using new bulbs, not necessarily good bulbs. A better test would be to take two lights that are working in another fixture and install them in the problem circuit. If they do not work, take them back to the original system and reinstall them to make sure they are still functional. This is a better, more robust test of the lights.

Example 3—hand injury during sandblasting: The first two examples primarily involve equipment; this example primarily involves people. The cause and effect tree in Figure 8 was based on this incident.

The incident description says the event occurred when the operators were sandblasting metal tanks in preparation for repainting. Each sandblasting machine was staffed with the normal two-person crew (a nozzle

Cause and effect tree for a lighting failure / FIGURE 6



operator and a blast-pot operator). When the nozzle operator observed that abrasive material was no longer flowing through the nozzle of his machine, he suspected a clog in the blast hose. He responded by releasing (disengaging) the dead man's switch, a switch automatically operated in case the human operator becomes incapacitated. The nozzle operator then signals to his co-worker, the blast-pot operator.

Assuming the system was depressurized, the blast-pot operator attempted to disconnect the blast hose from the equipment so he could clean away the suspected clog. The blast-pot operator was unable to rotate the quick-disconnect coupling the one-quarter turn required to remove the blast hose. Assuming the fitting was stuck because of dirt or contamination, he asked another blast-pot operator working nearby to assist him.

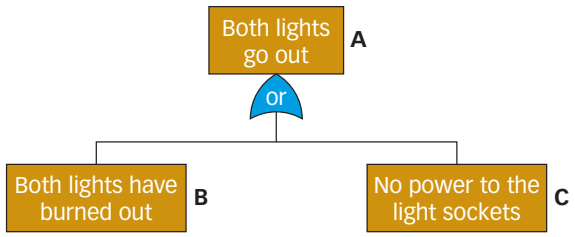
Acting together, the two blast-pot operators were able to twist the hose fitting to the point where it could be forcibly disconnected. The system rapidly depressurized through the opened coupling, spraying abrasive material through the coupling and onto the hands of the worker nearest the outlet, the first blast-pot operator. This worker sustained relatively minor, but painful, skin abrasions to both hands.

All workers were fortunate their eyes and faces were not injured, and the injured blast-pot operator was lucky his wounds did not become infected from the embedded sand.

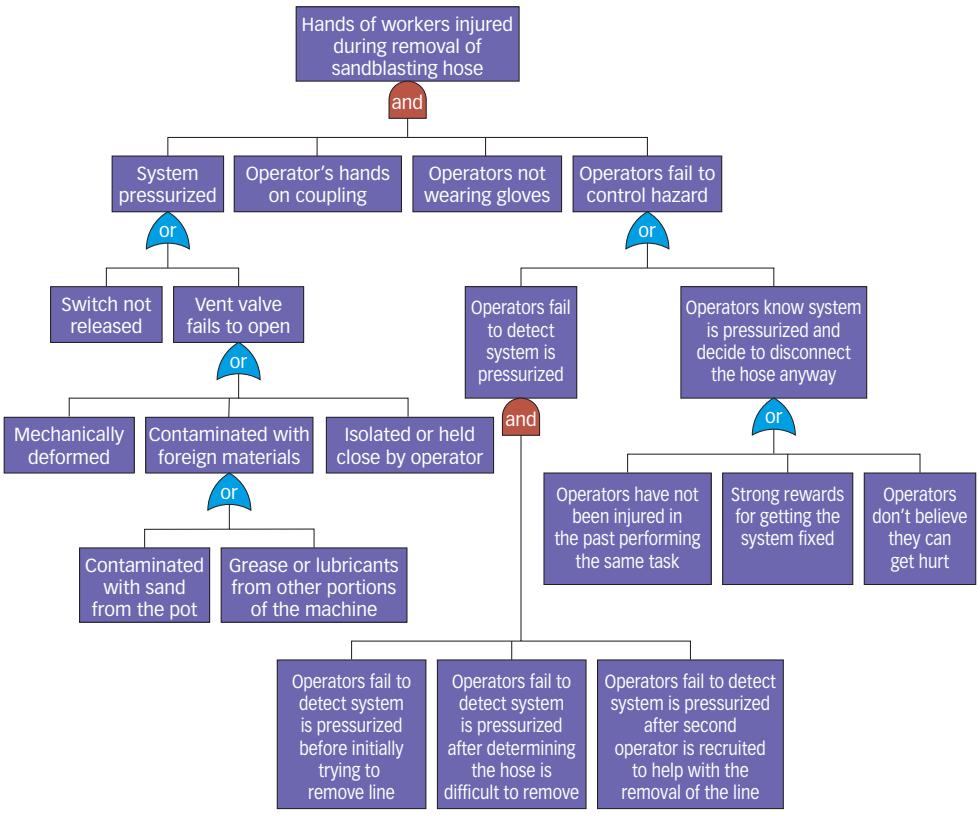
The equipment description is that the sandblasting machine involved in this incident is a relatively common piece of equipment. The machine consists primarily of a pot to hold abrasive material (similar to sand) and a flexible, 1-inch (2.5-centimeter) diameter blast hose to carry and direct abrasive material to the surface being cleaned. The machine is designed to be connected to a compressor and to operate at a pressure of 100 pounds per square inch (6.89 bars).

The pot can be pressurized and depressurized by the blast-hose nozzle operator using a pneumatic dead man's switch, which controls and synchronizes the opening and closing of the air inlet and outlet valves

Cause and effect tree with Events A, B and C / FIGURE 7



Cause and effect tree for hand injury during sandblasting / FIGURE 8



located on the pot. When someone engages the dead man's switch to start the sandblasting process, the air inlet valve opens, the outlet valve and the pop-up valve close to seal the pot, and the pressure in the pot forces sand through the blast hose.

When the dead man's switch is disengaged, the air inlet valve closes and the air outlet valve opens. This allows the pot to depressurize through the air outlet valve. When the pressure in the pot nears atmospheric pressure, the pop-up valve opens to allow more abrasive to be added to the pot.

The top event in Figure 8 is "Hands of worker injured during removal of sandblasting hose." For this to happen, four general events need to occur:

1. The system must be pressurized.
2. The workers detach the hose with the system still pressurized.
3. The operator's hands are on the coupling.
4. The operator is not wearing gloves.

All four events need to occur, so an "and" gate is used. If the system fails to depressurize but the users never take the hose off, they will not be injured in the way the top event describes. If the system is depressurized when they take the hose off, they also will not be injured. Finally, if the operators are wearing gloves, they will not be injured.

So why would they disconnect the hose with the system still pressurized? The cause and effect tree identifies two possibilities:

1. They did not detect that the system was pressurized.
2. They knew there was a hazard but decided they could disconnect the hose anyway.

Data are gathered to determine which branches are true and which are not. Interviews are performed and the equipment examined to determine which branches should be eliminated.

In this case, multiple causes may exist. Although it may end up being necessary to train personnel on how to determine whether the system is still pressurized, the employees may still not know that a pressurized system poses a hazard. Therefore, it might be necessary to address both of these potential causes, not just one.

In the second case, personnel knew there was a hazard but decided they could disconnect the hose anyway. Why would they decide to do this? The cause and effect tree shows three possible reasons:

1. The operators have disconnected the hose with the system pressurized in the past and have not been injured.
2. The operators are highly motivated to fix the system because of expected job rewards or penalities.
3. The operators don't believe they can get hurt in this situation.

If the first case is true, we need to ask why the improper behavior has not been corrected in the past. In the second case, we need to ask why an unsafe behavior has been encouraged. In the third case, we need to change the operators' perceptions of the risk. Of course, this incident will help change the injured operator's perception of the risk, but we also need to change other personnel's perception of the risk.

Visit www.qualityprogress.com for a continuation of this article, which covers the construction and drawing of a cause and effect tree. The online material includes examples of symbols and structures and a nine-step procedure, along with 21 additional figures. QP

JAMES J. ROONEY is a senior risk and reliability engineer with ABS Consulting, Public Sector Division, in Knoxville, TN. He earned a master's degree in nuclear engineering from the University of Tennessee. Rooney is a fellow of ASQ and holds the following ASQ certifications: biomedical auditor, hazard analysis and critical control point auditor, manager of quality/organizational excellence, quality auditor, quality engineer, quality improvement associate, quality process analyst, quality technician, reliability engineer and Six Sigma Green Belt.

LEE N. VANDEN HEUVEL is a senior risk and reliability engineer with ABS Consulting's energy division in Knoxville, TN. He earned a master's degree in nuclear engineering from the University of Wisconsin-Madison. Vanden Heuvel co-authored the Root Cause Analysis Handbook.

DONALD K. LORENZO is a senior risk and reliability engineer with ABS Consulting's energy division in Knoxville, TN. He earned a master's degree in nuclear engineering from the Georgia Institute of Technology. He authored A Manager's Guide to Reducing Human Errors: Improving Human Performance in the Chemical Industry *and is director of the Process Safety Institute.*

LAURA O. JACKSON is a risk/reliability engineer with ABSG Consulting Inc.'s public sector division in Knoxville, TN. She earned a bachelor's degree in nuclear engineering from the University of Tennessee.

THE TREE GROWS

The online continuation of this article explains how to construct a cause and effect tree using a nine-step procedure. This additional material, along with 21 more figures, can be found at www.qualityprogress.com.