Conduct an Effective Incident Investigation

Frederick T. Dyke
ioMosaic Corp.

Information that can reveal the root cause of an incident resides in many places — within the plant or process unit, and in control rooms, offices and witnesses' minds. Here's how to find the data and conduct effective witness interviews.

READERS WHO WERE LISTENING TO THE radio or watching television on the morning of February 1, 2003, will remember the loss of the Space Shuttle Columbia over Texas. Within an hour of losing contact with the Columbia, NASA's Mission Control declared a "contingency" to ensure that all mission data were preserved. All flight controllers had to verify that their logs were up-to-date and institute a hands-off policy with regard to switches, push-buttons, controllers, knobs and the like; all computer data were impounded. This was the start of NASA's incident investigation procedure.

Process plants need to develop similar procedures to be carried out following an accident. To successfully determine the root cause of an incident, it is essential to do a thorough job of locating and preserving all the available data and information. It is better to have too much data and too many interviews than to get to the end of the investigation and find that the one key piece of information needed to establish conclusively the incident cause is missing. This is why NASA declared a contingency in the Columbia incident that started with the preservation and collection of all data, not only at Mission Control in Houston, but also at the Kennedy Space Center and shuttle contractor facilities.

This article suggests actions to take following a large incident to preserve data and witness information. These same techniques can be scaled down for smaller events. Smaller incidents will involve smaller investigation teams and smaller areas of impact, but the same steps must be followed to preserve and acquire the data necessary for a thorough investigation.

It is hoped that none of the readers of this article will ever need to implement such a plan. However, plants need to have a plan — with roles and responsibilities clearly defined — in place.

Immediate actions

The plant staff should take the following actions immediately until the first members of the investigating team arrive at the site and can take over the investigation.

First, secure the accident site, including the process unit, the plant or unit control room, and offices. Close these areas to all personnel. Only members of the investigating team should be allowed access. If there was an explosion and debris is scattered, the debris field must also be cordoned off.

This must be done quickly. The investigation team needs time to get organized, assign responsibilities and prepare protocols for the collection and handling of data. If this preparation is rushed, data collection could be disorganized and much of the information gathered will become questionable.

Even before data collection starts, the plant staff must take steps to ensure that any sensitive or perishable records and equipment, such as computers and electronic instrumentation, are protected from exposure to the elements. Ensuring this has been done should be the investigation team's first priority upon arrival, even if it is not yet up to full strength and support services have not been organized to remove the records and equipment to a more protected location.

Data collection

The first place the team should look for data is the plant or unit control room where the control instrumentation is located. Note instrument setpoints and take a close-up picture of each recorder or indicator.

Photography

Photographs should be taken as part of the data gathering activities. Two photographic options exist — traditional photography with film, and digital photography.

Digital photography may present a problem, as digital images can be manipulated unless steps are taken to secure the digital media on which the original image is recorded. This requires establishing a chain of custody and providing a secure storage location for the original digital media.

A photographic negative has the advantage that it cannot be easily changed or manipulated. If a negative is wanted in digital form, it can easily be scanned and digitized.

Because of the potential questions that may be raised about a digital image, the best approach is to photograph the incident scene with a traditional camera. If a picture's authenticity is questioned, the negative can be produced.

Team members who are taking pictures should keep a log of all the photographs they take. They should record in this logbook the roll number, shot number, and subject of each shot (or the equivalent information about the subject of each digital image). The first frame of each roll should be of something (*e.g.,* a sign or a calendar and clock) that positively identifies the roll. If the camera has a built in date and time stamp, that feature should always be turned on. Lastly, when using a digital camera, never delete any picture files.

Some devices record more than one process variable using different-color inks. Make note of the ink colors and the process variable represented by each.

Next, examine the backs of the control panels and record the instruments' tuning constants (proportional band, reset and derivative).

After these steps have been completed, remove the charts from the recorders, label them, and save them. Do not save just the portion of the chart from a few hours before the incident. Save the whole chart, as the team may need to establish an operating history for several days or weeks before the incident. If a new chart was recently installed, check wastebaskets in the control room for the old chart. The unit foreman or chief operator may save the old charts for a period of time, so look in their offices as well. If they are not in either of these places, a dumpster search may be necessary.

While securing the charts, check the annunciator alarm panels and note any points in alarm. Take pictures of the annunciator panels.

After gathering the control panel data, the team should go through the control room and offices and collect the operators' and supervisors' log sheets and log books. This includes the outside operator log sheets that may be kept in the control room or at some location in the unit. Operator logs will contain notes on events that happened on each shift, repairs, equipment problems, materials movements, etc. Shift supervisor logs usually contain instructions to be relayed to the operators from plant management, such as operating conditions, feed rates, products, equipment to be prepared for maintenance, etc.

Next, the team should look for maintenance logs of work completed or in progress. Look for maintenance work requests and maintenance work permits. Permits are issued for lockout/tag-out (LOTO) procedures, confined space entry, line breaking, and hot work, among other things. This information can help to establish the condition of the plant and maintenance activities underway at the time of the incident. Permits are usually found in a supervisor's office or in the control room at the operator's station. Plants often require that a copy of the permit be displayed at the maintenance work site as well.

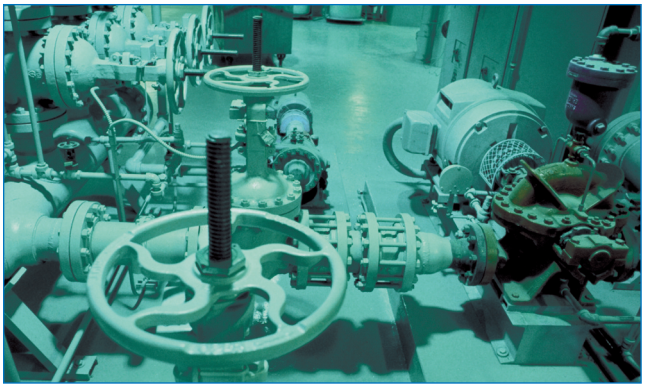
Many plants have computerized maintenance-management systems. These systems log and store a history of maintenance work performed on each piece of equipment and the associated costs. At a minimum, check the availability and security of the data.

If there is any doubt about the security of information, print it out and/or make a backup electronic copy of the data files. In addition, a chain of custody for the media containing the copy of the data files must be started and a

secure storage location established.

Laboratory analytical reports pertaining to the unit should be collected from the control room and the control laboratory, and secured. When gathering records in the control lab, check for samples that were submitted just before the incident occurred that have not yet been analyzed. Any unanalyzed samples must be impounded and a chain of custody established for them.

Lab reports can include quality control reports on the product or the in-process testing of streams; for a batch process, they may also include an end-of-step analysis that is needed before operators can proceed to the next step of the batch. These data may be stored on a computer system, and they should be handled as discussed above. Also look for certificates of analysis for the raw materials delivered



to the plant, which may be located in either the control laboratory or in the control room. Check both areas, and collect the certificates for a period of time before the incident as well.

Plant equipment conditions

The plant must be secured to establish how it was being operated at the time of the incident and the condition of the equipment. The positions of hand valves and control valves and of switches must be preserved until they can be recorded.

A common problem is that some switches and valves must be moved to ensure the plant is in a safe condition before the investigation team arrives on-site. If this is necessary, the plant personnel making the changes must accurately record all of their actions. This information cannot be left to someone's memory. When the investigating team is operational, this information should be turned over to them.

The team must identify the key plant equipment that was involved in the incident, as testing or inspection may be required later. Items such as instrument transmitters and switches that initiate shutdown interlocks or alarms, and final control elements, such as control valves, are candidates for testing. Other pieces of equipment, such as pumps, heat exchangers, vessels and piping, may also have been involved in the incident. Even equipment that has been subject to fire has stories to tell and therefore should not be ignored.

The team should tag all relevant equipment items so that they will not be disturbed. As the team walks through the plant, it should note the positions of control valves and actuated block valves to determine whether the valves went to their fail-safe position when the plant shutdown occurred.

Before any of the items identified for testing or inspection are removed, a secure storage area is needed. A procedure for establishing a chain of custody, as well as removal and inspection protocols, must also be in place. When items are removed from the plant, as large a segment as possible should be taken. Take pictures of the equipment in place, as it is being prepared for moving, and the actual move. Later, as equipment is being tested and disassembled, take pictures of each step of the testing and disassembly process.

If the incident involved an explosion, fragments will be located throughout a debris field. Once a mapping plan is in place, each fragment location should be mapped and assigned a unique identifier. The fragment should be photographed in place, and then it can be retrieved. A chain of custody for the fragments must be established starting with this first movement.

Basic process control systems

Today, distributed control systems (DCSs) and/or programmable logic controllers (PLCs) control many plants. These computer systems control the entire plant or large packaged units. They usually record and condense the operating data for storage on a hard drive or other device(s).

The data storage equipment must immediately be protected from damage. As soon as possible, the computers and storage devices should be removed to a safe, secure and dry storage area. This is to save all possible data, as it may not be immediately clear what information will be needed. Once the equipment is in a secure location, extraction of operating information can begin.

DCS and PLC systems employ software programs to run the process. These programs must be saved as well. It may be necessary to investigate whether the incident was caused by a software error or by corrupted software. The DCS and PLC also contain instrument configuration data, such as setpoints, alarm limits, instrument tuning constants, control algorithms, etc., which need to be recovered.

The DCS has one or more printers for printing alarms,

the responses taken to the alarms, changes made to instrument setpoints, and when an alarm condition returned to normal or cleared. These critical data must be saved. Do not remove only the pages available on the printer; also look for additional pages in the control room, in trash baskets and in the unit foreman's or chief operator's offices, and if necessary, resort to a dumpster search.

In an incident investigation, these data are critical, and the more records available, the better the investigation. These logs give a picture of activity in the plant, problems that may have occurred before the incident, most likely the actual time of the incident itself, and maybe what initiated the event.

Sampling process materials

Another critical source of information is fluids or solids remaining in the process equipment. Take samples of these materials. Before starting this work, a protocol for removing the samples safely and establishing a chain of custody, as well as a secure storage area at the proper conditions to prevent sample deterioration, must be in place.

When withdrawing the material from the equipment, take one large sample at each sampling location. Divide it into several smaller ones for analysis so that everyone performing the analyses will be working with the same sample. This eliminates the need to consider sample differences when comparing the analytical results from different organizations. If solids are present, special procedures are required to ensure a representative and uniform sample. Sampling will have to be coordinated with those team members looking at and removing equipment.

If samples must be transported from the incident site to an analytical laboratory, they may need to be shipped as hazardous materials. Someone trained in the regulations and procedures for handling and transporting hazardous substances should be available to the investigation team.

Develop protocols

Many types of information and data must be collected and secured following an incident. Before the information is gathered, a protocol specifying how this is to be done must be developed to ensure that no evidence is lost. This is important because it forces those collecting the data or performing the sampling to first think about what they are doing, how they are going to do it, and what they hope to gain from their efforts.

Generally a protocol should describe how the data are to be collected safely, such as requirements for personal protective equipment, information required during collection, what is to be done with the data or samples (*e.g.*, storage), and how the chain of custody will be documented. A testing protocol should describe how the testing is to be done and the data to be obtained. For example, it should spell out whether a technician taking apart a pipe should record the torque required to loosen flange bolts and the gasket type and its condition, and whether he or she should save the gasket. If parts are to be saved, the protocol should cover how the collected items should be tagged and numbered to identify what they are, where they came from, and where they should be stored.

Interviewing witnesses

Take initial witness statements after the site is secure and before staff and emergency responders leave the premises. The plant staff will have to do this because the investigation team will likely not be on-site. Taking statements immediately will yield more precise evidence, as the incident will still be fresh in the witnesses' minds.

Limit the initial statements to where the individuals were, what they saw, heard, smelled and felt, what time they think the incident occurred, and what they think might have caused it.

The investigating team can use the initial statements to plan in-depth interviews and decide whom to interview. Prepare a list of questions, general and specific, for each witness, and develop an interview schedule for both witnesses and interviewers.

Select a neutral and comfortable location for the interviews; avoid the offices of plant executives or managers. Have someone present whom the person being interviewed knows to help dispel the appearance of an adversarial relationship. Arrange the seating in a circle to further avoid the appearance of confrontation.

Interviews should be conducted by two people. One person should ask the questions and the other should take notes.

If regulatory agencies are conducting interviews, arrange to have an investigation team member attend and take notes, but ask no questions. These notes can be used as input to the team's interview process.

Before starting, explain the interview process and what will be done with the information to the witness. Assure him or her that every effort will be made to protect sources of information and that the use of names in the investigation report will be avoided.

Ask questions seeking personal information first, then general questions, then the specific incident-related questions. The final question should be: "Do you have anything to add or tell us?" Close the interview by reviewing the notes with the witness to be sure there are no misunderstandings.

After the interview, compile a written copy of the information learned from the interview. Allow time to prepare

this write-up in the schedule so it can be done while information is still fresh in the interviewers' minds. Allow the witness to review the write-up and to add comments or make corrections.

Share the information from the interviews with the other members of the investigating team. As a group, review interview results for contradictions among the witnesses — some are to be expected. Conduct follow-up interviews to reconcile significant contradictions, but avoid being confrontational.

Finally, remember that no matter how much time you plan for interviewing, it will always take longer.

A final word

By following these suggestions, the investigating team will be able to gather a complete set of incident data. Resist the temptation to jump to an early conclusion about the root cause of the incident and only collect data needed to support this conclusion. The Columbia contingency required that all possibilities be pursued until the data ruled something out. Adopt the same open-minded approach to your investigation. CEP

FREDERICK T. DYKE is currently a partner at ioMosaic Corp. (93 Stiles Rd., Salem, NH 03079; Phone: (603) 893-7009 x104; Fax: (603) 893-7885; E-mail: dyke@iomosaic.com), where he consults in the areas of process safety management, accident investigation, process hazards analysis and the design of pressure relief systems. Throughout his career, he has worked in many areas of chemical engineering, including inorganic and organic chemicals and batch and continuous processes, and has held assignments in plant operations, research and development, and engineering design. He has worked for Monsanto, W.R. Grace Organic Chemicals Div. and Arthur D. Little. He holds a BS and MS in chemical engineering from Northeastern Univ. (Boston, MA).