ioMosaic®

Minimizing risk. Maximizing potential.®

Best Practices For Saving And Protecting Critical Data Following An Incident

Part I

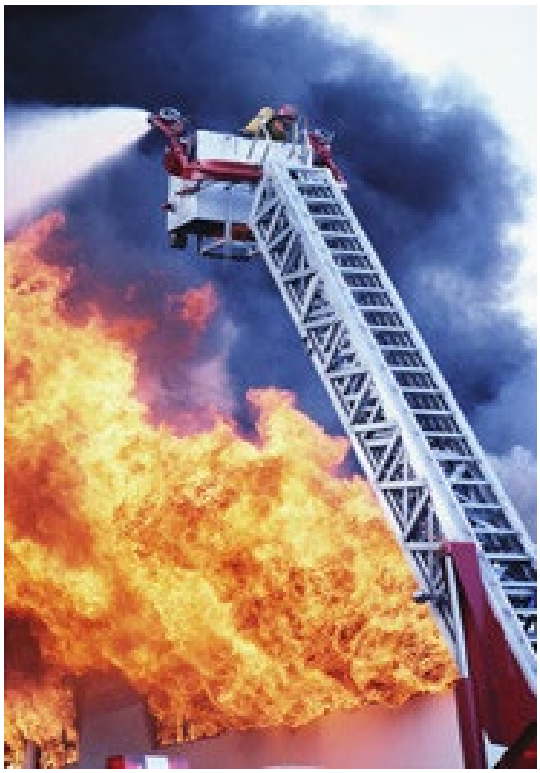
An ioMosaic White Paper

Introduction

Significant critical information is often lost following an accident/incident due to poor data and information gathering procedures. As a result, should litigation occur, information that could be useful in determining the cause of the incident and later in building a defense is not collected. This paper will try to overcome these possible problems and suggests some of the information and data that should be collected and saved following an incident.

First, only the data and information that will be useful for investigating the cause of the accident/incident is gathered. Therefore, the data and information needs for any potential litigation that could follow are completely overlooked. Second, an easy to use check list that identifies all the data that is available and required for collection may not be readily available. Last, the attorneys advising the client may not be aware of all the data and information available for collection, so they are unable to ask for it to be collected.

Immediately after an incident (either a major accident or environmental release) the first steps to be taken must be to protect information from further loss and to secure the incident area to prevent conditions of the facility from being changed. Additionally, the approach should be to save everything. Information that may not seem important initially can become critical to the incident investigation or for use in litigation defense to establish critical facts several weeks or months later.



The first place to look for data is in the plant or unit control room where the instrumentation is contained. First, the charts from the recorders should be removed, labeled and saved. These charts are usually rolls of paper or folded stacks of paper that move through the instrument. Save the entire chart. Do not just save the portion of the chart from a few hours before the incident. You may need to establish an operating history for several days before the incident. Also, if it is found that a new chart had been installed just before the incident, start checking wastebaskets in the control room for the old chart. The unit foreman or chief

operator may save the charts for a period of time, so look in their offices as well.

While securing the charts, have the team note the instrument set points. As this is done, also take a close-up picture of the recorder or indicator. Next, the team should go in back of the control panel and note the tuning constants, (proportional band, reset and derivative) for the instruments. Check the Annunciator alarm panels and note any points in alarm. Again, take pictures of the Annunciator panel.

While this is going on, someone else should go through the control room and supervisors offices looking for and securing the logbooks. Usually, operators have a logbook in which they note events that have happened on their shift, such as repairs, equipment problems, materials movements, etc. Shift supervisors logs will usually contain instructions the supervisors are relaying to the operators, or instructions that are given to the supervisor by plant management. For example, these could be actions such as preparing goods for shipment, products to be made, systems to be prepared for maintenance, or operating conditions to be used in the plant for example.

Another group of papers that should be collected is the material transfer logs or inventory reports. This will show movement of materials between tanks, tanks in use, and the amount of material stored in the tank, raw materials received and used, and product produced and shipped by the facility. As part of this collection, any shipping paper or bill of lading found in the control room or offices should be collected as well.

Next, the team should look for maintenance logs of work completed or in progress. This can include work requests and maintenance permits. Permits are issued for Lock Out Tag Out (LOTO) procedures, confined space entry, and hot work, to mention a few. This information can help to establish the condition of the plant and activities that were going on in the plant at the time of an incident. Permits may usually be found in a supervisor's office or the control room at the operator's station. Additionally, many plants require that a copy of the permit be displayed at the work site. All of this documentation must be gathered.

Many plants have computerized maintenance management systems. These systems log and store maintenance work performed on each piece of equipment as well as the costs associated with doing the maintenance work. At a minimum, a check should be made on the availability of this type of information and its security. If the security of the information is in doubt, it may then be necessary to have it printed out, or a backup copy of the data files made and given to the investigating team for later use. In this case, a chain of custody for the media containing the data must be established and a secure storage location found for it.

Laboratory analytical reports in the control room and those in the control laboratory that pertain to the unit involved in the incident should be collected and secured. These laboratory reports can be Quality Control reports on the product, in process testing of materials, or in batch chemical facilities an end of step analysis. In a batch procedure, the end of step analysis may be required before the operators can proceed. Again, this data may be stored in computer systems and it should be handled in the same way as the maintenance data detailed above.

The plant itself needs to be secured. To do this, it is important to establish how the plant was operated as well as the operation and condition of the equipment. This requires collecting information on the position of valves, hand and control, and switches for starting and stopping equipment. A major problem that is often encountered is that some switches and valves positions must be changed after the incident to ensure the plant is in a safe condition. If this is necessary, the individual(s) carrying out this work must record accurately any changes they make to the plant. This information can not be left to someone's memory.

Key equipment involved in the incident located in the plant must be identified, as later testing may be required. For instance, instrument transmitters that indicate process parameters and switches that can trigger automatic shutdown interlocks or alarms. Once identified, these components should be tagged. Other instruments to be concerned about are control valves. Following an incident, they have a failure position and it is necessary to determine if they moved to their fail-safe position when plant shutdown occurs. Some valves are meant to fail closed while others are meant to fail open. The valves identifications and positions as found in the field must be recorded. Key control valves that may require testing should be tagged initially for later removal and testing. This should also apply to safety relief valves installed in the plant that may require testing.

There may be pieces of equipment and piping in the plant that were involved in the incident. If at all possible, do not disturb these items until they can be inspected using a protocol for disassembly. If the items must be removed from the plant for safety reasons or they are in the way of reconstruction, have them removed to a secure location, in as

large a piece as possible, where they can be disassembled and inspected at a more convenient time. If the equipment is to be moved, then a chain of custody for the items should to be established. This also applies to any instrumentation that may be removed from the facility. Pictures of the equipment in the plant must be taken before removal starts. Later, as the equipment is disassembled for inspection, pictures of each step of the disassembly should be taken.

Today, many plants are controlled by Distributed Control Systems (DCS) and/or Programmable Logic Controllers (PLC). These are computer systems used to control the plant. These systems generally record data on plant conditions and store it on a hard drive(s) or some other kind of storage device(s). The equipment in which the data storage has taken place must be protected. The whole machine(s) that contains the storage system needs to be protected and removed to a safe, secure, and dry storage area as soon as possible. The reason to do this is to save all possible data, as it may not be immediately clear what information is needed. Once in a secure and safe place, work on extracting information from the storage devices can begin.

With the DCS and PLC systems are software programs for running the facility. These programs need to be saved, as it is possible they may have to be reviewed to determine if the incident was caused by a software error or by corrupted software. Also, there will be a program that is used to configure the instruments in the DCS. This configuration data is where set points, alarm limits, instrument tuning constants etc. are found

With the DCS system are also a group of printers for printing out plant data. At least one printer is used for printing out alarms, the actions taken on them, changes in instrument set points, and when the alarm condition returned to normal. This is important data and must be saved. They are worth securing, even if the printouts have been damaged. These logs will give a picture of activity in the plant, problems that occurred before the incident (most likely the actual time the incident occurred) and maybe what initiated the incident.

Ultimately, samples of fluids remaining in the process equipment should be taken. When this occurs one large sample should be taken at each sample location. A chain of custody for this sample needs to be established after the sample is taken. Also, suitable storage facilities for the samples must be provided to ensure that they do not change over time or get lost.

The reason for taking one large sample is that it can be divided into a series of smaller samples for analysis by all parties interested. By splitting the larger sample one can be sure that everyone has obtained the same sample too. This eliminates the problem of one party obtaining a slightly different sample with different results which can lead to all of the analysis being suspect.

If the incident involved is an explosion where there are fragments of the item that exploded spread around the site, these fragments should not be disturbed. Once a fragment location has been mapped, photographed, and then labeled with a unique identifier, it can be moved. However, a chain of custody for the fragment must be established starting with its first movement.

As mentioned above, many items must be photographed as part of data/information collection. Today there are two options for photography, the first is the standard photographic negative process, the second is to take digital photographs. The digital image may present a problem as these images can be manipulated unless steps are taken to secure the media on which the original image was recorded, establish a chain of custody, and a secure storage location for this media. A photographic negative has the advantage that it can not be easily changed or manipulated. If the negative is wanted in digital form it can be scanned and digitized easily. With the potential problems and questions that can be raised at a later time, the best approach for photographing incident information is to have a photographic negative. The negative can not be manipulated and can be produced if a picture's authenticity is questioned.

To overcome the problem of incomplete incident information, we have prepared a checklist. This checklist identifies major areas of data and information to be gathered. Also, this checklist is general enough to provide you with a starting place or to help prepare a detailed checklist tailored to an actual incident.

Please look for part II of this series on Incident Investigation dealing with how to conduct effective interviews after an accident has occurred.

Authors

1. Fred Dyke
2. Georges A. Melhem, Ph.D., FAIChE, melhem@iomosaic.com

Images

Source: Unknown/unidentifiable after good faith search. For educational purposes only. Not to be copied, shared or reproduced in any way.

Appendix A: Incident Data Saving Checklist

Control Room Instrumentation

- — Recorder charts collected
- — Controller set points, logged *(Photographed)*
- — Controller tuning constants, logged *(Photographed)*
- — Annunciator panel alarms, logged *(Photographed)*
- — Instruments for testing tagged

Note: for controllers located in the plant the same data as above must be collected.

Logbooks/Records

- — Operators log books collected
- — Field Operator logbooks collected
- — Shift Supervisors/Foreman's logbooks collected
- — Analytical laboratory sample log book collected
- — Material transfer/inventory records collected
- — Maintenance log books or files collected
  - a. Work orders
  - b. Permits for hot work, Lock-Out-Tag-Out (LOTO), confined space entry, line breaking, etc.
  - c. Equipment maintenance history records from files or computers
- — Personal protective equipment maintenance records collected
- — Plant safety equipment records collected

Analytical Laboratory

- — Raw material analyses collected
- — Raw materials certificates of analysis
- — In-process test results
- — End of step analysis
- — Final product analysis
- — Electronic records secure or copied and custody chain established

Plant Condition Changes

- — Control valve positions noted
- — Control valve changes recorded
- — Changes in manual valves
  - a. Positions recorded
  - b. Changes noted
  - c. Changes tagged
- — Changes in switches/circuit breakers for equipment
  - a. Positions logged
  - b. Changes noted
  - c. Changes tagged
- — Equipment to be inspected/tested tagged

Sampling

- — Secure storage location available
- — Chain of custody procedure in place
- — Large samples to be taken
- — Sample distribution log established

Computer Control Systems

- — All printer records secured
- — Software programs in use at time of incident download- ed. DCS and PLC
- — Operating data files secure or downloaded
- — Chain of custody for electronic data files and copies in place.

Explosion Location

- — Procedures in place to ensure fragments not disturbed.
- — Fragment mapping protocol established
  - a. Fragment identification method established
  - b. Location of each fragment recorded.
  - c. Location of each fragment photographed