How Instrumentation can reduce Hazards to People and Plant

Arthur Holland, Holland Technical Skills

On July 24 1994 around 8 am an electrical storm affected the power system at the Milford Haven oil refinery in the UK. In the following hours up to 1:23 pm, operators tried to keep the cracker running, aided by signals from the plant instrumentation system and VDU displays.
At 1:23 pm some 20 metric tons of liquid hydrocarbon burst through a pipe leading to the flare stack, formed a vapour cloud and exploded. 26 people suffered minor injuries and a van just missed entering an area that became enveloped in the fireball. Had it not been Sunday, multiple deaths would have occurred in the plant and injuries would have been expected in an area two miles away where shop windows were blown in.
Repair costs were estimated to be in excess of $80M and loss of production at several times that amount. An inquiry by the UK Health and Safety Executive revealed that the incident could have been prevented had operators diagnosed that the debutaniser outlet valve was stuck closed. However signals showing in the control room wrongly indicated that it had opened. Other flow signals implied that it was closed but operators failed to identify this inconsistency. While a number of detailed graphics were provided for individual sections of the plant there were no overviews of the complete process and alarms were coming in at one every two or three seconds.

As disasters go this is a small one but its lessons prompt us to look at practices and specific techniques applicable to the heat processing workplace.
“I could have told you something like that was going to happen”. This could be you talking, whether from management, engineering, procurement, plant design and manufacture, process technology, maintenance, production or plant operations. Any one of you could be in the line of fire when the coroner or a duly appointed inquiry person asks, “ Do you talk to each other? Did you report your concern?”

A major lesson here is that transparency is vital at all levels of the operation including cooperation of all the above mentioned people during specification, design, documentation, construction and start-up. The plant referred to here now has an $800 000 process simulator which is used to train operators and give them hands on experience of how the plant feels and responds in both normal and abnormal situations.

General recommendations

1.Make sure that your instrumentation provides both an overview and a detailed knowledge of the plant’s operating condition.
2. Have access to layout and schematic drawings and descriptions of equipment, wiring and piping with identification of plant items. Use these to evaluate the control and safety implications.
3.Check that you have ID labels on indicators, controls, internal cabinet wiring, terminals, piping and components. These include such simple matters as which switch position is OFF and which way is INCREASE on a manual controls.
4. Put in place procedures and priority rankings to be observed when responding to plant alarms and off-normal events.
5. Have stickers on cabinets and plant items showing manufacturer’s or outside supplier’s service phone numbers.

Specific examples
We will try to be specific by reference to some well-used techniques and examples. This involves applying your knowledge of your process, its instrumentation and monitoring to the challenge of heading off predictable hazards. Let's start with sensors.
.
Temperature sensor location
Ensure that your thermocouples or RTDs are located where they can see the temperatures of interest to you and that the wiring is sound. A misplaced or pulled-out-of-place sensor or one whose wiring is shorted can lead to overheating of the process.
Broken temperature sensor
In most processes you want a broken or burnt out (open-circuit) sensor to make your controller default to a high reading or "broken sensor" message and turn the heat off (sometimes called "upscale burnout"). If you don't specify otherwise, controllers normally come configured this way, being the usual safe default.

Some processes may require a broken sensor to default to full power or some predefined percentage of full power (sometimes called downscale burnout). If so, ensure that the controller is configured this way and this type is not mixed with upscale burnout controllers. Downscale burnout is used for example when you are trace-heating an outdoor pipe or a vessel that must on no account be allowed to cool off.

Reversed thermocouple
Thermocouple wires are often crossed when a process is being rewired or commissioned. This would normally send the controller indication downscale and call for full heat, perhaps damaging your equipment or making scrap product. Some controllers can recognize this as an unrealistic low temperature and default to power off or to the level of power that you specify.

Replacing thermocouples

Some plants have a mixture of different sensors and it is easy to take say a type R thermocouple off the spares shelf and install it where a type K came out. This would make the controller drive the temperature up to some three or four times the set value. So identify and label spare thermocouples and controllers by thermocouple type.

Auxiliary alarms on controllers

Besides the control output, a controller can have extra relay or logic outputs that can be configured as high, low, deviation high, deviation low or deviation band alarms; deviation that is, from the working set point. The usual convention is to have the relay or logic signal drop out in the alarm condition. This is usually defined as "fail-safe" because bad relay contacts and broken wires give a false alarm, reckoned to be preferable to an unrevealed alarm which the opposite logic would suffer. However, before you put too much reliance on the term "fail safe" you must thoroughly analyze the failure modes in any alarm, interlock or shutdown chain for loss of protection. For serious over temperature protection, remember that the controller could go bad so do not depend on the alarm circuit in the controller itself. You would be wise to provide a totally second opinion in the form of a separate alarm instrument or module on its own dedicated thermocouple or RTD.

Rate-of-change Alarm

There are times when you want to alarm on a fast moving temperature, for example to head off a large change or a thermal reaction. In these cases you would specify a rate-of-change alarm and set it in units of degrees/minute.

Load-break Alarm

With this feature the controller watches and times any movement of process temperature. At the same time it notes its command to its power output device, (a contactor for example) and looks for a contradiction. The controller will trigger an alarm in the following cases. The heater contactor is welded closed, ignores the controller's command to turn off and produces a rise of process temperature.

The heater is open circuit, ignoring the controller's command to deliver heat so the controller sees that the temperature is falling.

The temperature sensor is pulled away from the process heat and showing say, room temperature, yet the controller, seeing a low unchanging temperature, is commanding full heat.

There are other ways to pick up heater problems that do not depend on the time-out of a temperature change.

Solid-state-relay Monitoring

Some solid-state relays use the controller's turn-on logic signal wires to carry back a pulse-coded signal to the controller, representing heater current. The controller can pick up and alarm on two kinds of contradiction of these two signals.

1. The SSR has failed in the short circuit mode and is passing current in the absence of a turn-on logic signal. In this case the alarm can be used to kick off a back-up contactor.
2. The SSR has failed in the open circuit mode or the load circuit is broken so it ignores the turn-on logic signal from the controller. The alarm here would give early warning of loss of process temperature.

Latching Alarms
A process can go into alarm and out again while you are looking the other way. This is a non-latching alarm and you might not want to miss it.
Consider which alarms you want to configure as latching i.e. to stay active until you acknowledge and attend to the problem.
Indications
If you are to trust your picture of the plant you must pick up indications of plant condition directly from the parameter you want to monitor and not by inference from say the percentage output display on a controller or from its 4-20 mA output signal.
Two examples: you should be looking for a real heater current or a signal from a position feedback device on a valve stem. Be aware that broken or disconnected valve actuator linkages can deceive your display.
Units of measure
Dangers lurk in mistaking degrees F for degrees C and interchanging the various imperial and metric units on your displays. Import and export of equipment will always pose this threat until the world agrees on a common system.
Distributed Control Systems (DCS)
While the principles covered above refer to controllers, a DCS system would be functionally the same but with more comprehensive graphic displays and data analysis. There is an intermediate stage where controllers and indicators with communicating capability are integrated into a PC which becomes the user interface for display and operator manipulation. An advantage here is that the controllers can continue independently to control, protect and indicate if the computer goes off line or hangs up. Some operators feel more in control with this back up and the ability to isolate and exchange controllers and indicators.
Human-machine Interface (HMI)
This is where you can harm yourself and the process by not understanding the meanings of the settings, readings and parameter adjustments that you have to use. They are usually anything but natural and instinctive and it is possible to find yourself out of your depth and guessing. You have to insist on clear HMIs and user manuals when you buy equipment. Then you have to practice so that you know the results of any adjustments that you touch, especially those where you can manually override and defeat safety features. I would recommend a strong contribution at the design stage from operators and maintenance staff in respect of plant overviews, detailed displays, control manipulation and response to the unexpected.