Ensuring Effective Decision Support in a Crisis

By Maurice Wilkins, Yokogawa

Operator error during periods of abnormal operations has been put forward as one of the causes of many major recent incidents. But before we give humans a bad rap, incident reports suggest the problem often stems from poor procedures, inadequate training, and the lack of sufficient resources. In many cases, with the right skills and tools, a good operator can help avoid these situations.

Arguably, the most advanced decision support systems may be found in the aircraft industry. But even these can go wrong sometimes, and it comes back to the skills and training of humans to avoid potential disasters, aided by a standards-based approach.

Putting Humans Under Stress

Process control systems have evolved over the years to the point where we can measure, display, and alarm almost anything in almost any color. We can provide many different alarms on the same measurement, including various high and low values, as well as rate of change. We build operator displays that look artistically great, but can confuse the operator in an emergency. But when configured correctly, these alarms and displays can help rather than confuse. Unfortunately, we often don't use this system intelligence to benefit the process operator.

On March 23, 2005, there was an explosion in the isomerization unit of the BP Texas City Refinery, which at the time was BP's largest facility. The explosion killed 15 people and injured 170. The incident centered around the raffinate splitter.

BP's incident investigation, led by J. Mogford, issued a report showing several basic procedure-related errors, such as a level alarm acknowledged but not acted upon, a heat-up ramp-rate that was too fast, and operators trying start up the unit in manual when procedures indicated it should be in automatic. Moreover, operators turned on the burners before verifying liquid was circulating. Later, we will examine how a standards-based approach may have averted this incident.

Another clear example of operator overload happened on Sunday, July 24, 1994, when a lightning strike started a fire on the crude distillation unit at the Texaco Milford Haven refinery, which eventually led to an explosion on the fluid catalytic cracking unit (FCCU). Although the media put the blame on the lightning strike, the incident report stated, "These events, though significant in initiating a plant upset, were not the cause of the release and explosion that occurred five hours later. These consequences resulted from subsequent failures to manage the plant upset safely."

Luckily, although there were some serious injuries, no one was killed. Among many other things, the report cited bad alarm management, poor human-machine interface (HMI) display design, and a failure to follow procedures. For example, the report stated, "From the limited amount of alarm information relevant to the event, which was preserved from just one of the journals, it was seen that in the last 10.7 minutes before the explosion, the two operators had to recognize, acknowledge, and take appropriate action on 275 alarms. At times during the morning, operators were doing nothing but acknowledging alarms."

The report went on to say the chances of operators restoring control manually were reduced as the incident progressed due to them being overloaded by a "barrage of alarms." There were 2,040 alarms configured, 87% of which were high priority. During the incident, the operators had to cope with alarms coming in at a rate of one every 2 to 3 seconds, which resulted in many simply being cancelled. There was no evidence that a vital high-level alarm on the flare drum that went off 25 minutes before the explosion was ever seen.

In addition, the report indicated the FCCU HMI graphics were not designed in a way to help the operators control the process. Process data was limited and color use was confusing, so important data was not highlighted. Much of what was displayed illustrated the structure of plant equipment and had no relevance to operations. Critical procedures had fallen into disuse from lack of practice and documentation.

The Role of Procedures

These incidents show how the effective use of procedures is one of the key items in maintaining safe and reliable operations under all conditions. In fact, if configured correctly, well-planned alarms can trigger procedures in many abnormal situations, and a well-designed HMI can bring a developing incident to the attention of an operator in a timely manner.

For example, the airline industry is among the safest and most automated in the world. In fact, most modern aircraft could not fly without the use of computer guidance, yet procedures play a big part in the way aircraft are operated. Pilots need to go through many procedures before, during, and after a flight.

History suggests recorded procedures were introduced by test pilots in 1935 after the crash of a B-17 Flying Fortress in Dayton, Ohio. The B-17 was the most advanced bomber at the time, but the crash almost caused the program to be abandoned due to a gust lock still being engaged at takeoff. It was said that the plane was too complicated to fly.

In response, test pilots developed procedures for use during takeoff, in-flight, before landing, and after landing. Boeing eventually delivered more than 12,000 of the aircraft to the U.S. Air Corps, and they flew 1.8 million miles without a serious mishap. An example of the B-17 procedures is shown in Figure 1. Every type of aircraft from small private planes to the largest jumbo jet now use procedures for all aspects of the journey, and not following them could lead to a pilot losing his or her license, or worse.

APPROVED B-17F and G CHECKLIST

REVISED 3-1-44

PILOT'S DUTIES IN RED

COPILOT'S DUTIES IN BLACK

BEFORE STARTING
1. Pilot's Preflight—COMPLETE
2. Form 1A—CHECKED
3. Controls and Seats—CHECKED
4. Fuel Transfer Valves & Switch—OFF
5. Intercoolers—Cold
6. Gyros—UNCAGED
7. Fuel Shut-off Switches—OPEN
8. Gear Switch—NEUTRAL
9. Cowl Flaps—Open Right—OPEN LEFT—Locked
10. Turbos—OFF
11. Idle cut-off—CHECKED
12. Throttles—CLOSED
13. High RPM—CHECKED
14. Autopilot—OFF
15. De-icers and Anti-icers, Wing and Prop—OFF
16. Cabin Heat—OFF
17. Generators—OFF

STARTING ENGINES
1. Fire Guard and Call Clear—LEFT Right
2. Master Switch—ON
3. Battery switches and inverters—ON & CHECKED
4. Parking Brakes—Hydraulic Check—On—CHECKED
5. Booster Pumps—Pressure—ON & CHECKED
6. Carburetor Filters—Open
7. Fuel Quantity—Gallons per tank
8. Start Engines: both magnetos on after one revolution
9. Flight Indicator & Vacuum Pressures CHECKED
10. Radio—On
11. Check Instruments—CHECKED
12. Crew Report
13. Radio Call & Altimeter—SET

ENGINE RUN-UP
1. Brakes—Locked
2. Trim Tabs—SET
3. Exercise Turbos and Props
4. Check Generators—CHECKED & OFF
5. Run up Engines

BEFORE TAKEOFF
1. Tailwheel—Locked
2. Gyro—Set
3. Generators—ON

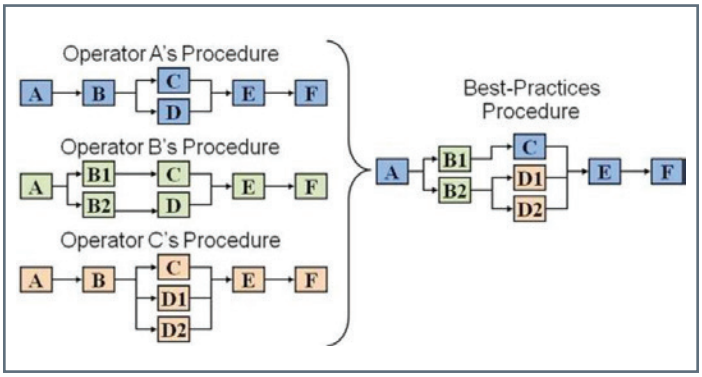
AFTER TAKEOFF
1. Wheel—PILOT'S SIGNAL
2. Power Reduction
3. Cowl Flaps
4. Wheel Check—OK right—OK LEFT

BEFORE LANDING
1. Radio Call, Altimeter—SET
2. Crew Positions—OK
3. Autopilot—OFF
4. Booster Pumps—On
5. Mixture Controls—AUTO-RICH
6. Intercooler—Set
7. Carburetor Filters—Open
8. Wing De-icers—Off
9. Landing Gear
   a. Visual—Down Right—DOWN LEFT Tailwheel Down, Antenna in, Ball Turret Checked
   b. Light—OK
   c. Switch Off—Neutral
10. Hydraulic Pressure—OK Valve closed
11. RPM 2100—Set
12. Turbos—Set
13. Flaps ½—⅔ Down

FINAL APPROACH
14. Flaps—PILOT'S SIGNAL
15. RPM 2200—PILOT'S SIGNAL

Another example of outstanding use of procedures is the now famous "Miracle on the Hudson." Captain Chesley (Sully) Sullenberger and his crew saved U.S. Airways flight 1549 on Jan. 15, 2009, when the plane struck a flock of geese just after takeoff from La Guardia airport in New York. They landed the plane safely on the Hudson. It turned out that none of the crew had flown together before, but the procedures drilled into all airline crew enabled them to do all the necessary things by rote.

In the process industries, we use standard operating procedures (SOPs) for all aspects of running a process, under all conditions. However, some of the better operators often tweak procedures to improve them. As experienced operators are retiring with often less experienced operators replacing them, plants try to capture these tweaks to develop best-practice procedures (see Figure 2).



These procedures can be run semi-automatically, where the control system runs the steps to a point where the operator must confirm it is safe to continue, or the control system runs the procedure completely automatically. The machine runs the process, but there is always a need for human oversight.

Experience Counts

Under normal conditions, humans operate very well, but as stress builds, people react in different ways. Some become heroes in wartime situations by giving leadership under fire, but in manufacturing we don't expect heroism.

Having several very skilled "operators" probably saved Qantas flight 32 on Nov. 4, 2010. The flight, using an A380 Airbus—the world's largest and most technically-advanced passenger aircraft at the time—had left Singapore for Sydney. Over Indonesia, one of the engines blew apart, rendering almost the entire wing controls inoperable and leaving only one engine to power the plane.

The pilots were inundated with messages: 54 came in to alert them of system failures or impending failures, but

only 10 could fit onto the screen. The pilots watched as screens full of messages came in. Luckily, there were five experienced pilots onboard, including three captains who were on "check" flights. Even with that much experience available, it took 50 minutes to work through and prioritize the messages.

The incident report concluded that without those pilots, the flight would probably not have made it. In fact, the "airmanship" of the pilots saved the plane. If the pilots had followed all the advice from the flight systems, the plane would have crashed. The most senior pilot told the others to read the messages but "feel" the plane. They managed to land safely with one working engine.

There are many times when the quick thinking of an operator has probably saved a process, but of course, these successes don't get the same publicity as aircraft incidents.

A Standards-based Approach

As stated earlier, modern control systems can have the versatility and intelligence to help an operator, but without guidance, these features can confuse as much as aid the operator, hence the need for standards (see Figure 3).

With an effective HMI display, an operator can easily see what state the process is in, and if an alarm is activated, it can be seen easily and acted upon quickly. But process alarms also can be used to trigger an automated action if configured correctly. The action can be a combination of informing the operator, taking corrective action, or even halting the process if needed.

The International Society for Automation (ISA), a globally-recognized standards development organization, has two standards and one in development addressing operator decision support:

- ANSI/ISA-18.2-2009: Management of Alarm Systems for the Process Industries
- ANSI/ISA-101.01-2015: Human Machine Interfaces for Process Automation Systems
- ISA106: Procedure Automation for Continuous Process Operations.

ANSI/ISA-18.2 provides requirements and recommendations for the alarm management lifecycle. The lifecycle stages include philosophy, identification, rationalization, detail design, implementation, operation, maintenance, monitoring and assessment, management of change, and audit. Using this standard should prevent incidents like the one at Texaco Milford Haven. Alarms are rationalized and prioritized so high-priority alarms either trigger an action automatically or ensure an immediate operator response.

ANSI/ISA101.01 is directed at those responsible for designing, implementing, using, or managing HMIs in manufacturing applications. The standard itself has internal standards aimed at producing an HMI philosophy, graphic style guide, and design toolkit- all of which should lead to an interface helpful to the operator.

The ISA106 committee has produced one technical report defining models and terminology, and is close to releasing a second report on work processes, before starting the steps of developing a standard. The standard will help define which procedures should be automated and under what circumstances.

When combined, these three standards offer powerful tools to provide decision support in times of normal and abnormal operations.

BP Texas City Done Right

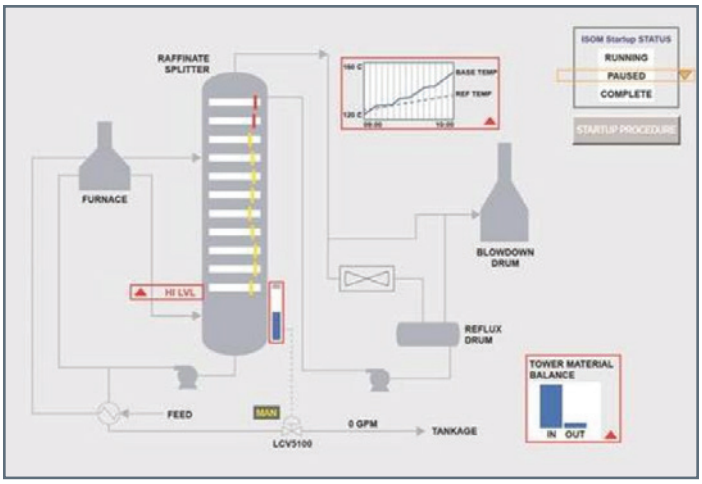
Returning to the BP Texas City incident discussed earlier, Figure 4 shows how the integration of alarm, HMI, and procedure management might have prevented the incident. Imagine what one of the operators could and should have seen on the control-room screens prior to the incident:

- The high-level alarm is tripped.
- The procedure is paused.
- There is a mismatch in the material balance because no liquid is leaving the column.
- The column temperature is significantly above the desired value.

All this information could have been used by the operator or an automated system to alleviate the abnormal situation, preventing the disaster that followed.

An effective standards-based decision support system can help improve process safety and provide critical aid to operators in times of stress, but more is needed. An effective decision support system should be able to:

- Draw on historical data for memory of what has happened in the past.
- Incorporate both data and models to analyze and present the best options.
- Assist operators in semi-structured or unstructured decision-making processes.
- Support, rather than replace, operator judgment.
- Aim at improving the effectiveness, rather than efficiency, of decisions.



In process industries, decision support of this nature is not yet widely available. But with the advent of less expensive and more powerful computers, enhanced decision support will be more widely used to predict impending events as they are developing, allowing operators to take corrective action.

Mary L. Cummings, former director of the Humans and Automation Laboratory at the Massachusetts Institute of Technology and a Navy F-18 pilot, has conducted research into human-automated path planning optimization and decision support. She observed: “Humans are doing a pretty good job, but they do it even better with the assistance of algorithms. This research is really showing the power of how, when algorithms work with humans, the whole system performs better.”

So, maybe there is a balance between humans and machines that can ultimately make all of us safer. Let’s try to find it.

YOKOGAWA

Co-innovating tomorrow®

Yokogawa Corporation of America
12530 W. Airport Blvd.,
Sugar Land, TX 77478

yokogawa.com/us

Yokogawa Canada, Inc.
Bay 4, 11133 40th Street SE,
Calgary, AB T2C 2Z4

yokogawa.com/ca

Yokogawa de Mexico, SA de CV
Urbina No. 18
Parque Industrial Naucalpan
Naucalpan de Juarez, Estado de México
C.P. 53370

yokogawa.com/mx