Apply *Can't* Rather than *Don't* to Your Process

William A. Levinson, P.E.
Levinson Productivity Systems

Many safety systems rely on human intervention to prevent incidents. A different approach is to make it impossible for a catastrophic accident to occur. Learn how to implement the *Can't Rather than Don't* principle.

Process safety can be viewed through many lenses. One perspective is based on *can't rather than don't*, a concept that originated at the Ford Motor Co. These four words encompass a universal safety principle: "In so far as it is practicable it is not a case of *don't*, but the installation of devices that stand for *can't*" *(1)*. Error-proofing devices apply *can't rather than don't* to discrete manufacturing operations; inherently safer technology (IST) *(2)* is equally important in the chemical process industries (CPI).

Don't refers comprehensively to vigilance, conformance to rules and regulations, and other forms of human intervention such as inspections and preventive maintenance. Traffic safety relies almost entirely on *don't*, as in "don't run stop signs or traffic lights, and don't change lanes without looking first." Conformance requires constant vigilance and attention from the driver. Stoplights behind tree branches, stop signs that have faded to white octagons, faded lane markings, and potholes are shortcomings of the *don't* approach. Heavy reliance on procedures to prevent accidents is why highways are generally far more dangerous than workplaces.

Can't, on the other hand, refers to devices, processes, or technologies that make accidents impossible regardless of a human's vigilance or adherence to rules or procedures. A punch press that can easily crush or sever a worker's hand is an excellent illustration of the difference between *can't* and *don't*. The combination of signs that warned "Don't put your hand in the punch press" and procedures that instructed workers to signal each other when ready to begin operation failed to prevent the loss of thousands of fingers and hands in American workplaces during the early 20th century. The Ford Motor Co. designed punch presses that require the worker to press two buttons, one with each hand, to operate them *(3)*. Instead of warning workers with don't-put-your-hand-in-the-punch-press signs, the manufacturer redesigned the punch press so a worker's hands can't be in the press when it closes. The accident then becomes impossible.

This article provides an overview of what *can't rather than don't* means for the CPI and discusses inherently safer technology in the context of this perspective. It also provides examples of some of the worst chemical accidents, including the Bhopal disaster, and how the failed safety systems relied on the *don't* principle.

Firearm safety

A simple example of the *can't rather than don't* principle is firearm safety. Consider the potential modes for carrying a semiautomatic weapon:

- Condition 0 — a round is in the chamber, the pistol is cocked, and the safety is off
- Condition 1 — a round is in the chamber, the pistol is cocked, and the safety is on
- Condition 2 — a round is in the chamber, the pistol is not cocked, and the safety is off
- Condition 3 — the chamber is empty, the pistol is not cocked, and a charged magazine is in the gun

Article continues on next page

Copyright © 2014 American Institute of Chemical Engineers (AIChE)

• Condition 4 — the chamber is empty, the pistol is not cocked, no magazine is in the gun, and the safety is off.

There is some disagreement among police officers and others who carry handguns for personal protection as to whether a semiautomatic weapon should be carried in Condition 1 or Condition 3. A weapon in Condition 1 can be fired quickly in an emergency, but it relies on *don't* rather than *can't* to prevent accidental or negligent discharges, *e.g.*, "Don't forget to put the safety on, and don't allow anything to get inside the trigger guard." The latter is especially true for a Glock, whose safety catch is built into the trigger itself. The weapon cannot fire unless its owner puts his finger inside the trigger guard — or, as reported in Ref. 4, a windbreaker's drawstring gets into the trigger guard.

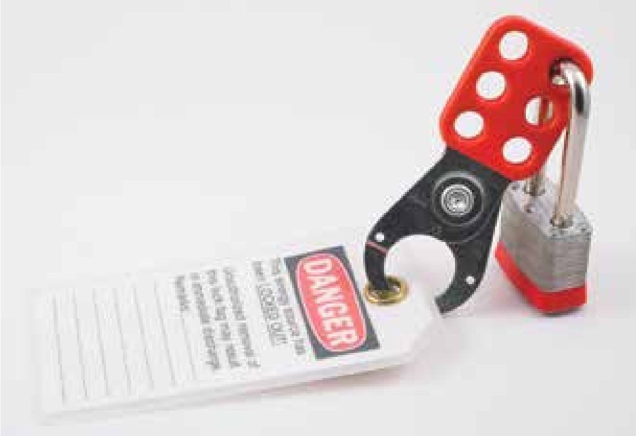
The punch press example illustrates the point that written procedures and warning signs are all examples of *don't*, while the Glock example suggests that many mechanical safety devices also rely on *don't* rather than *can't*. They make accidents less likely, but not impossible. Condition 3, on the other hand, makes it physically impossible for the weapon to fire, because the hammer is not cocked and there is no round in the chamber.

The M1911 automatic Colt pistol and its relatives are inherently safer because the user must depress the grip safety before the weapon will fire. The principle is similar to that of the Ford punch press, because the firing system ensures that the user is actually holding the weapon before it will discharge. Soldiers carrying the M1911 have typically done so in Condition 3 (at least during World War II). If the soldier needed to use it, he pulled the slide back to load a cartridge from the magazine into the chamber and also cock the hammer; that is, the soldier had to deliberately supply mechanical energy to make the pistol operable. Releasing the slide drove the cartridge into the breech, and the weapon could then fire.

Zero potential and lockout-tagout

A chemical process unit with no stored mechanical energy (including gas under pressure), chemical potential (*e.g.*, reactants), or electricity — which is the situation in a locked-out tagged-out activity — is similarly incapable of causing harm to maintenance workers. In lockout-tagout, each worker uses a lock for which he or she has the only key to secure the valves or switches of the equipment that is being worked on (Figure 1) — thereby eliminating the potential of anyone else restoring an energy source to the unit. Instead of a sign that says, "Don't open this valve," even if it is accompanied by a warning of disciplinary action for doing so, a lock proves unequivocally, "This valve can't open."

The need for all workers involved to remove their locks to restore power and utilities to a system in logout-tagout mode is equivalent to the requirement that both operators of a two-worker punch press push a total of four buttons to operate the press. If somebody is not where he or she belongs — *e.g.*, away from the equipment under maintenance, or out of the way of the punch press — the equipment can't function.



▲ **Figure 1.** Lockout-tagout requires each person working on a piece of equipment to attach his or her personal safety lock to secure the equipment, which cannot be operated until all locks are removed.

Inherently safer technology

A chemical process relies on the presence of chemical potential (kinetic and thermodynamic driving forces), and often on heat and pressure as well. It is still, however, possible to apply *can't* rather than *don't* in the form of inherently safer technology (IST).

A system is inherently safe when it is physically incapable of causing harm regardless of mistakes by personnel or unforeseen external circumstances such as natural disasters or even terrorism. (Chemical engineers tend to prefer the term inherently safer to avoid the implication of absolute safety and the absence of risk.) IST relies on the following *(5)*:

• *Substitute*. Substitute safe materials for dangerous ones. If the material is not hazardous, its release cannot endanger someone. Supercritical solvents involve high pressures, which are not desirable from an IST standpoint, but they can be used as alternatives to hazardous solvents. For example, supercritical carbon dioxide can be used in place of methylene chloride to decaffeinate coffee.

• *Minimize*. If a hazardous material is necessary, use smaller quantities of it, and consume the hazardous material as rapidly as it is produced. In that way, there will not be enough around to hurt someone in the event of a process upset, accidental release, or other incident.

• *Moderate*. Use less-intensive conditions, such as lower pressures and temperatures. At lower pressures, the system contains less mechanical potential, reducing the harm that can be caused in the event of equipment failure. Operating at lower temperatures reduces the rate of equipment degrada-

Copyright © 2014 American Institute of Chemical Engineers (AIChE)

tion, as well as the potential for fires and personnel burns.

- *Simplify*. Reduce process complexity. The *in situ* generation of highly reactive materials is viewed by some as a means of simplifying a process, although it also seems to be an example of minimization.

In many cases, substitution and moderation might not be practical (or possible). The Arrhenius equation states that chemical reactions will be faster, and productivity therefore higher, at higher temperatures. High pressures improve the conversions and/or yields of many gas-phase reactions. Chemical reactions work because the ingredients are, in fact, reactive, and anything reactive is almost certainly flammable, a health hazard, an oxidizer, and/or corrosive. The best course of action, therefore, is to have as little of these materials around as possible.

Don't in Bhopal

Consider the Bhopal disaster of 1984, in which the highly reactive and toxic methyl isocyanate (MIC) gas leaked from its storage tank, causing thousands of deaths and hundreds of thousands of injuries among people exposed to the gas. At the Bhopal complex, methylamine was reacted with phosgene to produce MIC, which was then stored before it was reacted in a second process with 1-napthol to form the final product, carbaryl. The disaster occurred when water entered the MIC storage tank and caused an exothermic runaway reaction. The temperature and pressure increased in the storage tank until a plume of the toxic gas was vented from the tank.

The plant had multiple safety systems to deal with a discharge of MIC, and all of those safety systems had to fail for the release to occur. As discussed in the article preceding this one ("Consider the Role of Safety Layers in the Bhopal Disaster," by Ronald J. Willey, pp. 22–27), that is what happened. Any one of several safety measures might have prevented, or at least lessened the impact of, the disaster.

Unfortunately, those layers of protection were based on *don't*: Don't overfill the storage tank. Don't allow the temperature and pressure in the tank to exceed their alarm setpoints. Don't disable the refrigeration system. Don't allow any MIC that leaves the tank to escape into the atmosphere. Don't take the flare system out of service, or don't operate the plant if the flare is out of service. Anything that relies on human activity, or lack thereof, constitutes *don't* rather than *can't*.

If, on the other hand, MIC was produced only as rapidly as the downstream process consumed it *(6)*, it would not have been present in any appreciable quantity, and the catastrophic release could not have occurred regardless of the activities of plant personnel or the condition of the safety-related systems. This does not make it acceptable to disable safety-related systems or fail to maintain them, but it does make a major disaster impossible even if all the safety systems fail.

Just-in-time production

A process in which the reactor sets the pace for the generation of the dangerous reactant(s) is similar to what discrete manufacturers call just-in-time (JIT) manufacturing, pull-production control, or kanban. Nothing is made until it is needed, whereupon it is used immediately. This approach is practical for other hazardous, but commercially important, chemicals, such as chlorine and phosgene.

On Jan. 23, 2010, at the DuPont facility in Belle, WV, a worker was exposed to phosgene, and subsequently died from the exposure. According to the U.S. Chemical Safety and Hazard Investigation Board (CSB), a braided steel hose connected to a 1-ton capacity phosgene tank suddenly ruptured, releasing phosgene into the air, spraying the worker in the face and torso *(7)*. The American Chemistry Council Phosgene Panel recommends against the use of hoses constructed of permeable cores and materials subject to chlorides corrosion for phosgene transfer. The more important detail of this incident, for the purpose of this article, is the 1-ton capacity of the phosgene tank. The ability to store a ton of phosgene makes *don't* the only obstacle to a disaster.

Generating phosgene on an as-needed basis eliminates the need to keep large quantities of it on hand, which changes the situation to *can't*.

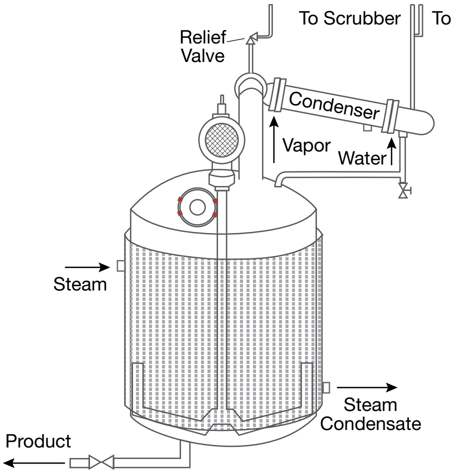
Continuous flow and IST

On Aug. 28, 2008, a tank exploded at the Bayer CropScience facility in Institute, WV, claiming the lives of two workers *(8)*. The explosion occurred in a 4,500-gal pressure vessel (residue treater), which was designed to decompose methomyl in a heated methyl isobutyl ketone solvent. Under normal operations, the vessel is prefilled with solvent and heated before dissolved methomyl and other waste chemicals are fed into the tank. However, on the night of the explosion, the methomyl solution was pumped into the residue treater before it was prefilled with clean solvent and heated to the minimum operating temperature. This caused a runaway decomposition reaction of methomyl, which generated too much gas for the emergency vent system to handle.

The takeaway from the Bayer CropScience tank explosion is that, whereas batch reactors rely heavily on *don't*, continuous-stirred tank reactors (CSTRs) and plug-flow reactors (PFRs) support *can't*. Batch reactors are generally more susceptible to human and automatic control errors, along with process upsets. A CSB video related to the incident discusses the reactor startup, and notes that 2,200 gal of flammable and toxic material had accumulated. These words — startup and accumulated — remind us that a batch reaction begins with all reactants at maximum concentrations.

CSTRs and PFRs, on the other hand, do not accumulate large quantities of material. A CSTR operates at the lowest concentrations of its unused reactants (*i.e.*, the composition

Copyright © 2014 American Institute of Chemical Engineers (AIChE)



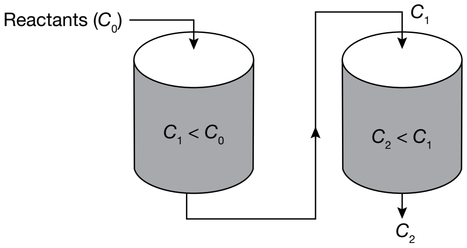
▲ **Figure 2.** In a batch reactor, the reactants are at their highest concentrations upon startup.

of the product stream), while concentrations drop rapidly in a PFR. A PFR offers far greater surface area than a jacketed batch reactor, which means removal of reaction heat is much easier and more controllable.

Henry Ford applied the principle of continuous flow to discrete manufacturing processes: "We can no more afford to carry large stocks of finished, than we can of raw, material. Everything has to move in and move out" *(9)*. This is exactly what happens in a CSTR, PFR, or fluidized-bed reactor — everything moves in and moves out.

Production control managers in discrete-manufacturing industries can attest to the drawbacks of batch processes. Batches accumulate inventory and increase cycle time. They also give defects a place to hide — that is, if nonconforming pieces are present in a batch, they will not be discovered until the factory workers inspect or use them. When units are produced and used one at a time, nonconformances become immediately obvious. (A batch of discrete widgets cannot, however, explode like a batch reactor full of chemicals.)

On Jan. 31, 2006, an explosion destroyed Synthron's chemical manufacturing facility in Morgantown, NC, causing one fatality and a dozen injuries. The explosion occurred in a 1,500-gal batch reactor, in which acrylic monomers were polymerized in the presence of two flammable solvents, toluene and cyclohexane. The polymerization reaction generated significant heat, which was removed by condensing the solvent vapor in an overhead, water-cooled condenser. The cooled, condensed solvent then flowed back into the reactor, keeping the temperature and the reaction under control. However, on that day, the company scaled up the polymerization recipe to fill a higher-than-usual customer order — more than doubling the energy release and overwhelming the cooling system. According to the CSB, the explosion was the result of a runaway chemical reaction in the polymerization reactor.



▲ **Figure 3.** With two CSTRs in series, the concentration of the reactants in the first CSTR never exceeds the concentration in the product stream (C_1), and the concentrated reactants with a concentration of C_0 are added only as rapidly as they are depleted by the reaction.

The CSB identified contributing factors such as inadequate maintenance, inexperienced personnel, failure to perform a process hazard analysis (PHA), and lack of features to detect and mitigate a runaway reaction *(10)*. All of these considerations are variations on *don't*. Don't forget to perform the maintenance; don't assign untrained and inexperienced personnel to the operation; and don't forget to watch for warning lights on the control panel. On the other hand, eliminating any significant quantity of the reactive materials will turn *don't* into *can't*.

Consider Synthron's polymerization reactor shown in Figure 2 *(11)*. The reactant concentration is initially at its maximum of C_0. (This refers to the initial concentrations of all the reactants, *e.g.*, C_{A0} and C_{B0} if there are two reactants, A and B.) Thus, the reaction rate is at its highest when the reaction begins, and the reactor's entire volume is occupied by this concentrated solution. However, the fact that the product can be withdrawn from the batch reactor as a suspension or a solution suggests that a series of relatively small, and easily controlled, CSTRs could be used instead (Figure 3). The reactant concentration in the first CSTR equals that in the exiting product stream, which is much lower. Instead of mixing large quantities of concentrated reactants at the beginning of the reaction, they can be added only as rapidly as they are consumed.

Referring to the Synthron accident, the CSB makes a strong argument for limiting the quantity of concentrated material that is present at any time. "Polymerization reactors can runaway with disastrous consequences if they are not carefully controlled. In a runaway reaction, the pressure, and thus the boiling temperature, in the reactor increases, further increasing the rate of reaction, and leading to higher pressures and heating rates" *(11)*.

The Five Whys

No single article can cover all possible aspects of personal and process safety, but The Five Whys — an iterative problem solving technique from the quality management profession — can be enormously helpful.

The Five Whys technique involves asking "Why?" until

Copyright © 2014 American Institute of Chemical Engineers (AIChE)

you reach the root cause of a problem. Consider the Synthron accident. The Five Whys could proceed as follows:

1. Why did the polymerization tank explode? Because the cooling system did not keep the reactor temperature in check.

2. Why did the cooling system not work as designed? Because more heat was generated in the reactor than the cooling system was designed to handle.

3. Why was more heat generated in the reactor than normal? Because more monomer was loaded in the reactor than normal. Thus, the reactor was operating outside of its design capacity.

This technique does not necessarily consist of five questions. Sometimes the root cause is identified in fewer questions and sometimes more are needed.

The Five Whys can be modified to identify good situations, as well as the causes of bad ones. In an ISO 9001 quality management audit, for example, instead of asking, "Are all of the gages in calibration?," you would ask, "Why is it impossible to have a gage in your factory that has missed its calibration?" The answer might be that gage management software alerting shop personnel that a gage is nearing its calibration date prevents this. Because this is an example of *don't*, the technique would continue by asking, "Why is it impossible for operators to not respond to software alerts?" A procedure that tells workers to check the calibration stickers of the gages they are using might technically satisfy the requirements of ISO 9001 but, because it relies on human vigilance, it is still an application of *don't*.

When applied in this way to *can't* rather than *don't* situations, the Five Whys only requires one question and one answer. Here are some examples:

- Why can't the punch press crush a worker's hand? The worker must have both hands on the control buttons, which are safely away from the press, before it will function.
- Why can't I connect an oxygen tank to a pipe that carries flammable material? The threads of the connectors are designed intentionally to not fit.
- Why can't this reactor or storage vessel explode, destroy a significant part of the plant, and/or kill workers? There is never enough reactive material present to do that kind of damage.
- Why can't a home generator electrocute utility workers who are working on a nearby power line? A transfer switch makes it impossible to connect the home power system to the generator and the public power line at the same time. A panel interlock switch serves the same purpose.

Ask why until you get an answer. If there isn't an answer to why the incident can't happen, safety depends on *don't* instead of *can't*.

Each of these examples has an immediate answer to a single why as opposed to a series of questions and answers. This brings up yet another important point. When you ask why to find the root cause of a problem, several questions may be necessary to get to the root cause. When you ask why to determine why an incident can't happen, more than one round of questions suggests there might be complexity in the safety system. A simple solution is almost universally better than a complex one when it comes to safety, as long as it is effective and comprehensive. CEP

WILLIAM A. LEVINSON, P.E., is the owner of Levinson Productivity Systems (6 Lexington Court, Wilkes-Barre, PA 18702; Phone: (570) 824-1986; Email: wlevinson@verizon.net). The company specializes in quality management and the application of Henry Ford's proven principles to manufacturing and service operations. Levinson received a BS in chemistry from Pennsylvania State Univ., an MEng in chemical engineering from Cornell Univ., and night school degrees in business and industrial statistics from Union College. He is a Fellow of the American Society for Quality, and a life member of AIChE. He is a licensed professional engineer in Pennsylvania. (Nothing in this article constitutes formal engineering advice.)

Literature Cited

1. **Norwood, E.,** "Ford: Men and Methods," Doubleday, Doran and Co., New York, NY, pp. 84–93 (1931).
2. **U.S. Chemical Safety and Hazard Investigation Board,** "Inherently Safer: The Future of Risk Reduction," www.csb.gov/videos/inherently-safer-the-future-of-risk-reduction/, CSB, Washington, DC (2012)
3. **Resnick, L.,** "How Henry Ford Saves Men and Money," *National Safety News*, p. 8 (Sept. 13, 1920).
4. **Sanchez, R.,** "Drawstrings Can Cause Guns Many Law Enforcement Agencies Use to Fire," *The IndyChannel*, www.theindychannel.com/news/call-6-investigators/drawstrings-can-cause-guns-many-law-enforcement-agencies-use-to-fire (Mar. 6, 2014).
5. **Hendershot, D. C.,** "Inherently Safer Design: The Fundamentals," *Chem. Eng. Progress*, **108** (1), pp. 40–42 (Jan. 2012).
6. **Edwards, V. H., and J. Chosnek,** "Make Your Existing Plant Inherently Safer," *Chem. Eng. Progress*, **108** (1), pp. 48–52 (Jan. 2012).
7. **U.S. Chemical Safety and Hazard Investigation Board,** "DuPont Corporation Toxic Chemical Releases," www.csb.gov/dupont-corporation-toxic-chemical-releases/, CSB, Washington, DC (Jan. 23, 2010).
8. **U.S. Chemical Safety and Hazard Investigation Board,** "Inherently Safer: The Future of Risk Reduction," http://youtube/h4ZgvD4FjJ8, CSB, Washington, DC (July 11, 2012).
9. **Ford, H., and S. Crowther,** "My Life and Work," www.gutenberg.org/ebooks/7213, Doubleday, Page and Co., Garden City, NY (1922).
10. **U.S. Chemical Safety and Hazard Investigation Board,** "Final CSB Report on Synthron Explosion Finds Inadequate Safety Controls for Chemical Reaction Hazards," www.csb.gov/final-csb-report-on-synthron-explosion-finds-inadequate-safety-controls-for-chemical-reaction-hazards/, CSB, Washington, DC (July 31, 2007).
11. **U.S. Chemical Safety and Hazard Investigation Board,** "Case Study: Runaway Chemical Reaction and Vapor Cloud Explosion," www.csb.gov/assets/1/19/Synthron_Final_Report1.pdf, CSB, Washington, DC (July 31, 2007).

Copyright © 2014 American Institute of Chemical Engineers (AIChE)