Thinking About Safety

January, 2001

Control Technology Corporation, Hopkinton, MA • 800.282.5008 • www.ctc-control.com

When working with industrial machinery, the possibility of human injury or significant economic damage is ever present. Any good manager, when asked if the safety of his employees is his primary, overriding concern, would, of course, say "yes" without hesitation. It is, however, an unfortunate and sometimes tragic fact that safety is not always granted this top priority in the original design of industrial machinery.

The purpose of this Technical Note is to provide some additional thoughts on the subject of safety in the original design of industrial machinery. It is not intended to be an exhaustive treatment of the subject, nor can it replace the professional judgment of a qualified design engineer in insuring the safety of a new design.

The Designer's Responsibility

The primary responsibility for insuring the safety of an industrial machine lies with the machine's designer. There are several compelling reasons for this fact:

1. Only the machine designer is cognizant of the forces involved in the machine's actuators.
2. Guards, backup systems and inherent safety features are all part of the task of designing a new machine.
3. The machine designer is responsible for the selection of components and materials that are appropriate for the application.
4. Part of the machine design task is an assessment of how a machine will be used; the level of expertise of the machine's operators, and the potential for the misuse of the machine.

An experienced design engineer realizes the danger of assuming that everything will work as intended, that component failures will occur under controlled conditions (or not at all) and that the operator of the machine and maintenance personnel will perform their jobs flawlessly Nowhere does Murphy's Law work as well as in the area of safety assurance.

Many of the safety practices that, at first glance, might seem absurd arise from actual experiences in which human injury was sustained. Sometimes this was due to an obvious danger in the worker's environment, but sometimes the cause was merely a moment of poor judgment or loss of concentration on the part of the worker. However we may feel about such circumstances, the legal responsibility for such injuries often bears on the designer of the industrial machinery involved.

As a practical matter, the only defense in such a situation is to be able to show that all prudent design precautions were taken to insure a safe machine, and that safety was in no way compromised as a primary design goal.

A Word About Reliability

Things break. This seemingly obvious fact is sometimes clouded by wishful thinking in the hectic pace of a design project. Castings may contain hidden flaws, metals may exhibit fatigue due to unforeseen stresses, electronic systems may be subject to statistical component failure, air valves may stick, etc., etc., etc.

Even in a machine designed with extreme care and attention to detail, unanticipated environmental factors (including excessive temperature or humidity, presence of chemical vapors, or faulty maintenance practices) may contribute to the early failure of system components. And, glowing statements about "reliability" in advertisements for components must be taken with a grain of salt (sometimes with a bucket of salt!). There is a reason why even so-called "fault tolerant" systems are not called "fault-proof."

Much of the task of insuring the safety of a new machine consists of paying attention to the "What Ifs . . . ". What if a mechanism breaks under stress? Will the machine's operator be injured as a result? What if the machine's control system falls? What if there is an electrical power failure, or loss of air pressure, or the breakage of a hydraulic hose, during the machine's cycle? Anticipate component failures, and put your design skills to work in finding creative ways to address their consequences.

We have heard of one instance in which a controller running a bottling plant, made by one of the industry's leaders (with a reputation for reliability), failed in such a way as to turn on all of its control outputs. This caused every actuator in the system to simultaneously turn on. Although fortunately, no injuries were sustained, the economic damage due to downtime was substantial. 'Me cause of the problem? It could have been a component failure within the controller, a problem with the AC power coming into the plant, someone dropping a wrench into the controls cabinet... Without anticipating the possibility of such a failure, the company was left susceptible to the damage which eventually occurred.

How can the effects of such failures be minimized? One technique involves the use of backup systems; systems capable of detecting faults and safely halting the operation of the machine in some overriding manner.

Some Guidelines for Backup Systems

A backup system is a system designed to protect against the failure of one or more components in a machine, usually by controlling the consequences of such a failure. A backup system may be as simple as a chain connected to a 2000 lb. hoist so that, if its mounting bolts fall, it won't come crashing down on someone's head. Or it can be as complex as a multimillion dollar computer installation which is automatically switched into Operation if it detects a failure in a primary computer system. In each instance, an assessment must be made of the possibilities for failure, the consequences of that failure and the effectiveness of the backup system in controlling those consequences. Some of the principles that are often used in the design of such systems include:

1. The backup system should be completely independent of the primary system that it is monitoring. After all, if the primary system falls, the backup system must still be active!
2. A different technology is often used for the backup system. For example, an electromechanical switch or relay is sometimes used in backup safety systems for programmable controllers. The reason for this is that the environmental factors that adversely affect electronic systems are different from those that affect electromechanical systems. (The bolt of lightning that damages the primary controller may also simultaneously damage any similar backup controller).
3. The backup system should be at least as reliable as the primary system, and there should be some means of insuring that it is always operational. If the backup system fails after one month without forcing maintenance to repair it, a subsequent failure of the primary system will be unprotected.

4. Sometimes, the above guidelines point to using a very simple device as a backup system. Dropout relays, interlock switches and mechanical guards are examples of widely used techniques.

In addition, specific measures are typically required by the nature of the machine being designed. Once again, a careful assessment by a responsible design engineer is the only answer.

Power Failure Considerations

One possibility, which cannot be ignored, is the eventuality of a power failure affecting the machine being designed. Machines can often develop substantial inertias in some of their moving elements. Often, electrical braking systems are used to overcome these inertias. What happens if power falls in mid-cycle? Will the braking system still work? Is there potential for injury or damage?

What happens if a machine's operating sequence is interrupted in mid-cycle? Will the power failure cause all of the machine's actuators to retract instantly? What injury or damage could this cause?

Chemical processes often involve critical monitoring of temperatures and careful control over valve timing and sequencing. What impact could a power failure have here?

One method of guarding against such a power failure is the use of "uninterruptible power supplies", which provide backup power in the event of loss of primary power. It should be noted, however, that even these systems are Susceptible to failure. Nothing takes the place of a machine design that is inherently safe.

Inherent Safety vs. "Added-on" Safety

It should be obvious that the time to start thinking about safety is during the original "conceptualization" of a machine's design. As machines become more complex, the old practice of designing a machine and then bolting on some guards to make it "safe" is no longer appropriate (if, indeed, it ever was). Thought should be given to how the operator will interact with the machine. For example, a stamping press where the operator will be manually placing a workpiece under a fast-moving press presents a dangerous situation. Even if guards and a two-hand anti-tie-down switch are used, the potential for injury due to malfunction still exists.

Thought might be given to methods for placing the workpiece automatically, perhaps using a pick-and-place mechanism (these are becoming surprisingly inexpensive) or some other transfer or shuttle mechanism.

Such techniques might not only improve safety, but also provide the added benefit of greater production rates!

Control strategies should also take safety into account as a primary, original design criterion. For example, a design for a massive hydraulic press involved two cylinders (12 inch bore!) welded to a common ram. The cylinders were actuated using proportionate control valves linked into a servo control system that maintained synchronization between them. If, however, any one of eleven separate system components were to fail, the cylinders could get out of sync, effectively tearing the machine apart.

In this instance, a separate differential counter was used to track the error between the two cylinders, sensing their position via encoders. If the cylinders, for any reason, lost synchronization, this counter drops out a master relay that removes power from the hydraulic power unit, stopping the system. An alternative strategy for protection, having a more direct correlation to the symptoms of pending failure, might have been to use strain gauge sensing of the stresses involved, or to apply something as simple as a tilt switch attached to the press's ram.

In any case, it was recognized early in the design process that special control requirements existed to insure safety, and steps were taken to incorporate protective measures into the control system's design.

The Designer's Safety

Contrary to popular belief and widespread practice, design engineers are not immune to accidental injury. In fact, they are frequently at substantially greater risk, due to the fact that they are working with partially completed machines, often lacking the safety systems that will be subsequently added as the machine is completed.

The design stage is, in fact, one of the most dangerous. Wiring, plumbing and software efforts may exist, unanticipated system incompatibilities may be present and flaws or inaccuracies may exist in machined parts that could cause sudden failure or erratic operation.

This imposes a special responsibility on the design engineer for his own safety. A constant awareness of the dangers inherent in the machine under design must be present, and actions that compromise the designer's safety must be avoided. If at all possible, tests should not be run on the machine until the intended safety and backup systems are installed.

Safety and Corporate Politics

We all live in a world where "economic realities" have an ever-present impact on the decision-making process. GO/NO GO decisions on machine design projects often hinge on "return on investment" (ROI) criteria set by the corporation. Safety requirements must be addressed in the budgeting process for a new machine and this, unfortunately, could have an impact on the viability of the project.

There should be an awareness during this decision making process, however, of the true impact of a strong safety program. For example, most companies are subject to safety audits by insurers, who determine the amount of risk imposed by the company's processes and equipment. Companies with a demonstrated concern for safety, as evidenced both by their practices and by their claim history, will fare well in this evaluation and reap substantially lower rates as a result.

Further, the restraints imposed by meeting safety requirements often result in a higher level of automation than was otherwise planned. This can create an offsetting benefit that should be taken into account.

There may come a time, however, when a severe compromising of the safety of a design would be necessary to make it "cost-effective" and thereby gain approval. When this point is reached, a wise designer (likewise, a wise manager or corporate officer!) will decide to move on to a different problem to solve.

The Good News and the Bad News

The good news to be derived from a thorough analysis of the safety issues involved in machine design is that many ways can be found to improve safety through intelligent, creative and careful design practices. For design engineers, safety assurance must be a principal part of their job definition, and must be taken into account in every design decision made. Safe, efficient and effective designs can be achieved, and new tools are becoming available each day to accomplish that end.

The bad news is that one careless decision can result in catastrophe; for a machine's operator, for your company and for you. Because the stakes are very high, the issues must not be subject to compromise or neglect.