

Unintended Consequences

Nelson L. Baxter, Contributing Editor

During the course of working in the industrial environment, I have noticed a distinct change during the last few years. The workplace has taken on an atmosphere of zero risk in the areas of safety and security. Much of this is the result of government regulation. This zero-risk approach has made it difficult to perform the daily tasks that are necessary to keep things running. It has resulted in what could in some cases be called politically correct, zero-risk paralysis.

All activities contain a degree of risk. What those who spew out regulations do not understand is that the unintended consequences of piling on more and more layers of regulation can create situations that are more dangerous than what the original regulatory act was designed to solve.

When designing a product, it is normal practice to weigh the costs versus the benefits. This simple common-sense approach never seems to take place *when* regulations are put into place.

An example of not doing a thorough study of all the effects of imposing a regulation was recently encountered at a power plant that involved the use of fire-retardant clothing. The safety people in charge mandated that all employees would have to wear FR2-rated fire-retardant clothing *no matter what job they performed*.

This meant that personnel working in hot locations who might have to also wear environmental suits were expected to comply with this rule. What the people who invoked this mandate failed to take into account was that the danger of heat stroke, because use of such heavy clothing in this situation far outweighed any benefit for this particular job task.

The work that my team and I perform while doing vibration surveys involves climbing hundreds of steps and walking several miles a day. In hot areas, especially during the summer, this type of clothing is a hazard. We are not exposed to either electricity or open flames, so it does not really protect us, but actually endangers our health due to overheating. If such common-sense reasoning is brought up to those in charge, you are considered “uncooperative” because you question those in charge of safety.

The problem here is that it's easier to paint with a broad brush and just make everybody do the same thing than it is to customize programs that recognize that what helps one work group perform their tasks more safely can actually endanger another work group.

Another example of safety overkill creating a worse problem involves installing

cages and guards on machines that make it impossible to measure the vibration levels. Those in charge of taking such actions should look at what happens when a high-speed machine comes apart due to a failed component. They might then realize that it is safer to let the doctor check the health of the patient than to prevent him from doing so. Inexperienced safety personnel evidently do not know the difference between a rotating shaft and a bearing, so they just cover everything up.

Another example of pursuing zero risk involves security. Security at plants has increased significantly over the last few years and has become a sacred cow that no one will challenge. The exterior security is understandable, because for their own safety, the safety of others and the need to not have operations compromised, it is necessary to limit who comes on a job site. Everyone agrees that this is necessary. However, there has been a recent push to lock more and more areas down within plant sites themselves. To justify their existence, there evidently are security consultants who feel the need to “ratchet up” security.

To do this, they start internally locking down more and more areas of the plant. A personal experience of mine involved starting up a large 550-megawatt turbine generator. My job involved being out next to the turbine monitoring vibration and listening for seal rubs or unusual sounds, monitoring growth of the casing and looking for steam or oil leaks. This diagnostic work involves constant movement between the turbine and the control room. It seems odd that I was entrusted with the health of a \$100 million dollar machine, but was locked out of the control room.

Every time I needed to get in, it was necessary for the operator to leave his control board and allow me to enter. This type of situation is equivalent to locking the doctor out of the hospital because he might do harm to the patients. If the doctor is trusted enough to treat the patients, then he should have access to them.

Locked doors everywhere also pose a distinct hazard when an emergency occurs. The locking up of more and more areas seems to be something that has a life of its own, since this approach is becoming more widespread. It may have the appearance of more security, but because of the unintended consequences of slowing down the implementation of operational actions and access during emergencies, it can result in a less safe environment.

A third example of restrictions that lead to unintended consequences involves Inter-

net security. For years, I worked in the field of remote machine diagnostic monitoring. This was very promising technology in that it allowed vital machine health information to be sent to experts so that they could evaluate the condition of the equipment and provide early warning of impending problems prior to failure and the associated consequential damages and downtime that result when a small problem grows into a big one and a machine totally fails.

The technology was available, but one of the most difficult problems to solve was that IT departments did not want to allow outside organizations to access the machine vibration data because of security concerns. This is another perfect example of how fear ended up in a knee-jerk reaction that prevented a promising technology from developing.

I remember in the study of history how knights would put armor on themselves and their horses, hold heavy shields and then go out to battle in the hot desserts. They felt safe behind their armor, but when they got into battle they could not see nor hear well and they and their horses would drop in exhaustion due to heat as their foes in lightweight clothing and swords outmaneuvered them and outlasted them in battle.

When at a facility and I cannot hear due to hearing protection, cannot see to my left and right because of side shields, am about to expire in thick clothing due to overheating, cannot get into the control room to tell the operators that they have a bad seal rub and cannot take measurements on a high-speed fan because someone has covered the bearings with a guard, I begin to identify with the knight.

Most of us responsible for operating, diagnosing problems and maintaining the facilities that make it possible for modern society to exist cringe at what the regulators are going to come up with next. Inexperienced politically appointed bureaucrats that have the power of law to make regulations and are not accountable for evaluating the unintended consequences of their actions have become a curse.

Most of the laws regarding safety and security were made with good intentions and have produced some good results, but implementing these laws is often heavy handed and counterproductive in both the areas of overall safety and security.

As the title suggests, this editorial is about unintended consequences, but they do not all have to necessarily be bad. Difficulties getting onto job sites, walking from machine to machine with most of our senses deadened by protective gear, being blocked from


performing testing in locked out areas and guards that prevent access to machines all provide a positive push to the installation of more on-line monitoring systems. Because of cyber security, these systems will most likely be monitored by in-house personnel to minimize the fears of the IT departments. This is the main point of this editorial.

The zero-risk policies of safety and security are making it more and more difficult for personnel to get anything done. It seems to be getting worse and worse with time.

To protect the large machines that make modern life possible, ratcheting up of safety and security may be the force that finally results in the tipping point that will make on-line monitoring a common approach to machine health monitoring.

One of the most common phrases we hear is the "upcoming internet of things." All our devices from our washing machines to our cars will be communicating over the Internet to tell us when they need maintenance. The need to keep personnel out of harm's

way by bringing data to them instead of them going to collect the data may indeed be one of the unintended consequences of this avalanche of regulations and security concerns.

We can all at least hope that something positive will come out of the regulations that now stymie our abilities to do our jobs effectively. 

The author can be contacted at: nelsonbaxter@att.net.