Session No. 537

Controlling Human Error in Complex Manufacturing Systems

Theodore W. Braun, MBA, CSP, CPE
Liberty Mutual Group
Hopkinton, MA

Introduction

Automation, a term that came from the auto industry, was initially used to describe relatively inflexible mechanized systems that controlled one or more machines and the means of conveying work pieces between the machines. Numerical control (NC) was a term used to describe the process of controlling a machine tool, originally using a tape or punch cards like the old computers. Today's automated equipment uses state of the art computer technology for automation and machine control. Technology and automation advancements are evolving rapidly and the modern industrial plant reflects the evolution with ever more complex systems and ever more difficult challenges to provide an acceptable level of safety.

Human – Machine Interaction

Human beings tend to want to be in control of machinery and not let the machinery control them. Human - machine interactions are highly variable and are affected by personal factors such as familiarity with the technology, uncertainty about processes and procedures, comfort with computers, knowledge of the systems, culture, language, age, education level, innate patience, and experience. Interactions are also driven by human factors engineering. Information display characteristics such as symbology, labeling, character readability, location, conformance with stereotypical expectations, and consistency with characteristics of input systems can affect the efficiency of normal production operations but might also have disastrous implications when a system malfunction is occurring. Similarly, human factors deficiencies with input devices such as levers, switches, buttons, knobs, pointing devices, can be problematic as well. The proliferation of complex and rapidly changing systems coupled with the factors affecting human machine interaction variability are a breeding ground for catastrophic injury. The frequency and severity of injuries is often related to the degree to which we fail to recognize human variability and take steps to control it.

Technology-driven systems are subject to the same learning curve problems as any human interaction. (Ott and Campbell, 1979.) Error rates tend to be high at first when the new technology is introduced and then decrease as we learn to operate the system. However, research appears to show that there is a finite minimum error rate. (Duffey and Saul, 2003.) Recognizing that there is a finite error rate and considering the amount of kinetic and potential energy in automated systems, the onus is on the designers, vendors, integrators and users to establish reliable safeguarding systems that are forgiving of error.

One of the major contributors to the automation evolution is the Programmable Logic Controller (PLC). Hardwired or wireless, these units are becoming ubiquitous. A recent change in NFPA 79 allowing safety PLCs having redundancy and reliability to replace hard wired safety relays creates both opportunities and threats for driving down risk on the production floor. Before this change, machine or automated system operation and machine safety were "wired" differently. State of the art computer systems would be used to provide the operational flexibility needed for quality and productivity whereas old style electromechanical systems would be used in parallel for safety functions.

PLCs take an input signal, process that input and send output signals to machinery based on the programmed ladder logic within the PLC. Input signals may come from simple microswitches, temperature sensors, position sensors, counters, two-hand control devices, light curtains, laser scanners, vision systems, proximity devices, etc. The list is nearly endless. PC-based CNC machine tool controls typically use "M" and "G" code commands to direct machine operations and, more recently, the PC systems can run other manufacturing operations as well. Systems can now be designed where the logic of the machine production operations can be directly integrated and monitored along with the safety functions. Computer controlled machinery and automated systems create huge risks but also potentially major benefits with respect to data for the safety practitioner. Why both the risks and benefits can be huge becomes clear with an understanding of the sources of injuries when working with automated equipment.

Studies conducted in the U.K. and in France show that the consequences of automation-related injuries are severe – nearly half resulting in permanent disability or death. (Vautrin and Dei-Svaldi, 1989.) Workers might be trapped and crushed against fixed objects, entangled with the equipment, caught in a point of operation, snagged by an end-effector, or a host of other types of crushing, shearing, and impact hazards. But how does this happen with state-of-the-art equipment designed to minimize human involvement, and in fact, to replace many of the more menial and repetitive tasks formerly performed by humans? A look at the types of tasks people are performing when injured, along with an understanding of the causes of human error, provides insight on why the injuries occur and what can be done to reduce the risk.

Not surprisingly, some injuries come from standard production operations where the system design did not account for all production tasks. Most suppliers of automated equipment feel it is their customers' responsibility to identify tasks, perform appropriate risk assessments, and then communicate their safeguarding needs. Automation suppliers do not typically tell their customers what they should do, so the onus is on the customer to design safety devices and controls into the process. Problems can arise not only from an incomplete risk assessment but also because there is such an assortment of safety devices and equipment from which to choose. Companies can look to outside consultants for advice on strengths and weaknesses of the various types of devices and controllers, but the decision is always made in-house on what will actually be done.

Most automation injuries come from three main areas, (1) machine maintenance, (2) machine set up and adjustment, and (3) reacting to operational disturbances such as jams or out of position parts. (Vautrin and Dei-Svaldi, 1989.) Those injured most often are machine operators and maintenance personnel. Too often, safety systems are designed with all the focus on safeguarding the standard machine operations, i.e., protecting the machine operators while maintenance activities are ignored, presumably on the assumption that maintenance will establish lockout and zero energy state whenever they work on the machine. This assumption is problematic because there is such pressure to get the system back up and running that shortcuts are taken and operators intercede to correct machine disturbances. The presence of accident risks during maintenance and

disturbance recovery operations may occur when the operator simply cannot avoid the risk, such as stepping over something that might be a tripping opportunity or when the operator can avoid the risk such as by shutting down the machine but elects not to. (Toulouse, 2002.)

To analyze the risks associated with production and maintenance tasks, we can use the guidance provided in ANSI B11TR3 *A Guide to Estimate, Evaluate, and Reduce Risks Associated with Machine Tools*, which outlines how to perform task-based risk assessments. A risk assessment uses estimates of injury likelihood and potential severity as inputs to categorizing risks that occur when performing a specific task.

Risk Assessment and Human Error

Task-based risk assessment on complex machinery or a cell of integrated equipment is a time consuming process, particularly when there is a great deal of flexibility with regard to work in process, production requirements, tooling, parts, wrapping, etc. Those who undertake risk assessment often focus strongly on the normal production and set-up operations because there is usually a great deal of detail already available from value stream mapping or similar types of analysis, but injuries tend to come from tasks that might be infrequent or even freak occurrences and not be identified in process improvement methodologies. It is important that risk assessments identify the infrequent and reasonably foreseeable system disturbances along with maintenance, set up, and adjustment tasks that might need to be performed when the machine is powered up. Examples include responding to a roll of plastic that is misfeeding, an out-of-alignment part or pallet, a palletized or conveyorized object that has fallen off, or a carton that has become lodged or jammed in a feeding system. When observing workers responding to system disturbances in automated systems, it is common to see some confusion with respect to safety systems, controls, and lock-out requirements. It is also common to see frustration and even anger when problems continue to arise.

A confounding aspect of the risk assessment process comes from recognizing that some individuals intentionally bypass a safety system. When undertaking a risk assessment, particularly where the severity of potential injury is high and there are reasons to go into the hazardous areas fairly frequently, the assessment team should identify how the system might be bypassed intentionally. Some systems are more fool-proof than others and the better solutions must be considered.

Many injuries are the result of human error. Why do people make errors or mistakes? We can gain insight from studies of vehicle accidents. Distraction, poor visibility, going too fast, lack of familiarity with the road, failure to see or respond to signals, fatigue, poor habits, alcohol and drug use, lack of familiarity with vehicle controls, stereotypical response, and multi-tasking are just a few of the reasons for the errors of omission and commission that cause accidents not only on our highways but also in our factories. There is nothing to be gained by arguing about whether or not people should be careful and not make errors. Everyone errs and we must accept that and design accordingly. When performing the risk assessments, the objective is to identify opportunities to eliminate the errors, reduce the likelihood of the errors, and reduce the severity of the outcome when an error is made. This is best done through system design, although behavioral approaches can be complementary activities. Some points to consider are:

- Is the system designed to make errors virtually impossible? This requires those who analyze the risk to consider the possibility that individuals will intentionally circumvent safety systems such as using a magnet to defeat an interlock switch.

- Is the system designed to make errors extremely remote? The focus is on avoiding unintentional errors such as those that might occur because of fatigue from extended shifts or frustration from frequent production interruptions or delays.
- Do the controls and displays operate according to stereotypical expectations and have labeling that conforms to the users' frames of reference?
- Are the controls located where there are clear lines of sight to all system components?
- Is there a natural pattern to the layout of controls and associated systems so that interaction is fluid and sequential.

Errors can be categorized as errors of omission and errors of commission. An error of omission is failing to do something that should have been done. An example of an error of omission is failing to remove the key from the switch that controls an interlock. By leaving the key in place, anyone can turn off a vital safety device and place themselves or others in jeopardy. There are many different types of errors of commission, the most common being sequential errors, extraneous errors, qualitative errors, and time errors. A sequential error is performing a step out of sequence. Energy lockout procedures generally follow a sequence of steps. If one were to throw the main switch before shutting off the machine, there is a much greater likelihood of an arc flash or blast. An extraneous error would be if the person were to throw the wrong main power disconnect. A qualitative error would be if the switch lever was moved only part way. In the process of conducting risk assessments, these typical types of human error must be factored into the analysis. One cannot assume that each step in a well-conceived process will be followed correctly. What we often consider to be ideal controls for a specified risk do, in fact, have many possible deviations from what is considered correct. Most of our systems are designed so that one, or even a few, deviations will not result in a catastrophic injury. With highly complex automated and integrated systems though, the number of potential deviations in following correct procedures is compounded.

Earlier, the comment was made that computerized systems can be a huge source of important data for the safety professional. Just as the systems gather production data, they can also capture data regarding the number of times an e-stop was pushed, an interlock opened, a keyed switch turned, etc. These uses or interruptions of safety systems can provide good information on how often system disturbances occur or operations conducted with a bypassed interlock. These data are invaluable for investigating error-prone situations for interventions before an injury occurs. To a safety professional, the data is similar to knowing about near misses (or near hits) which provide an opportunity to proactively address a risk. This data is complementary to operator interview information regarding the system disturbances that occur on the machine when operators should be describing the actions they take to intervene and correct the problems.

The best means of reducing error likelihood is to eliminate the source – to eliminate any reasons for the individual to expose themselves to a risk. If elimination is not feasible, the next step is through engineering solutions that reduce injury risk through physical barriers or interlocked (category 4) guards that keep the workers from entering a danger zone, or by redundant safeguarding devices that shut the system down and keep it from starting while a worker is in the danger zone. Warnings, work methods, education, training, and behavior controls would follow according to the commonly accepted hierarchy of controls. But on complex systems, a simple application of the hierarchy of controls can give a false sense that the risk has been reduced to an acceptable level. It is important to remember that complex systems may have opportunities for injury that result from poor human factors design of control panel layout or the computer

interface. Perhaps the location and accessibility of controls is an issue. Many systems have keyed interlock overrides and keys are left in the switches for convenience. Perhaps the ability to lockout all or sections of the automated system (electrical, hydraulic, pneumatic, etc.) is poorly designed, cumbersome, relatively inaccessible, or the power source feeds more than one machine or section of the system. Perhaps there are issues with interrupting a program in mid execution or putting the system in a manual override condition. Only a detailed risk assessment looking at each of the sub-tasks can reveal these types of issues that can lead to intentional and unintentionally overriding the safety systems. Operators must be involved in identifying the subtasks involved in disturbance recovery to fully understand not only the process but also the pressures they are under to get the system back to a normal state. (Backstrom & Doos, 1995.) Accident prevention requires that error-control solutions be developed that either eliminate production disturbances when those disturbances involve risk or act on the risk itself to reduce that risk to an acceptable level. (Toulouse, 2002.)

Human Error Control and Machine Safeguarding

The general approach to take with regard to safety devices and systems should follow this outline using the risk assessments as a basis for decision making:

1. Physically mark or outline the perimeter of the automated manufacturing system. Consider whether a perimeter safeguarding system is appropriate
2. Break the system into discrete zones with logical transitions from one zone to another. Then consider means and capability of isolating and safeguarding each zone so that the other zones can continue to operate while one zone is shut down and worked on.
3. Look at each piece of equipment/component, be it the production tool, parts transport devices, or parts positioning machinery. Each should have appropriate safeguarding related to the tasks and risks identified. Guard design and means of attachment, or device design and means of control, must be commensurate with the likelihood of injury and the severity of injury should one occur.
4. Look at entry points and locations where someone might be within the system while performing some maintenance, set-up, or disturbance recovery activity. Consider presence sensing devices such as mats and laser detection systems to keep the system from operating when individuals are in a risky circumstance.
5. Consider the control systems for the safety devices. Are they reliable and redundant electromechanical systems and Safety PLC systems? Do you know whether the program execution will be adversely impacted by power brownouts or voltage supply irregularities? Check with control system vendors and manufacturers on power supply issues that might impact input and output signals as well as the programming.
6. Carefully consider the start up process as well as the process for restarting when in mid program. It may be necessary to test the system at different points in the execution of the program(s) to check that the safety controllers are not allowing the unit to restart when someone might be in a danger zone.
7. Human interaction devices such as pendants, keypads, switches, knobs, other controls, and information displays should conform to good human factors design principles. Issues such as grouping, color, size, shape, conformance with stereotypical expectations, and accessibility should be considered.

8. Review the person-machine communication systems including status indicators and alarms, mode indicators, and systems that sense and communicate when individuals are in hazardous positions. (Aghazadeh, 1998.)
9. There may be some design risks that are not feasibly addressed through engineering. Consider the use of warnings and labels. Active warnings such as lights and sounds are better than simple cautionary signs. Safety labels should conform to appropriate standards (ANSI Z565.4.)
10. Design and deliver effective safety training around residual risks. Typically, there will be extensive operational training on the automated system and it is important that the safety training be integrated with the operational training and not be delivered as a stand-alone program. The task-based risk assessments will provide important insights into what the training program should cover.
11. Carefully audit the response to machine operating disturbances such as jams. Consider each step that the operators and maintenance personnel follow and identify what might happen if a step is performed out of sequence, incompletely, or not at all. Seek ways to reduce the number of steps and to make errors less likely or even impossible.

Conclusion

Automation and technology will continue to evolve on the plant floor, making production operations more efficient and escalating productivity. Automation does have risk but each risk can be addressed systematically with effective safety controls that allow people to operate and maintain the equipment safely. It is important to recognize that human beings make errors and these errors can be catastrophic when made in an unforgiving automated system. At first view, automated systems appear to be so high-tech that one might conclude that they are extremely safe. The approach to dramatically improving automated system safety is to identify error-likely situations, particularly when operators are involved in disturbance recovery, and to reduce the likelihood through a combination of human factors design and appropriate levels of safeguarding.

Bibliography

Aghazadeh, F., Chapelski, R., and Hirschfeld, R., A hazard analysis system for robotic work cells, Human Factors and Ergonomics in Manufacturing, Vol. 8 (4) 323-330, 1998.

Backstrom, T., & Doos, M. A comparative study of occupational accidents in industries with advanced manufacturing technology. The International Journal of Human Factors in Manufacturing, 5, 267-282, 1995.

Duffey, R.B., & Saull, J.W. Errors in technological systems. Human Factors and Ergonomics in Manufacturing, Vol. 13 (4) 279-291, 2003.

Ott, K.A., & Campbell, G., Statistical evaluation of major human errors during the development of new technological systems. Nuclear Science and Engineering, (71) 267-279, 1979.

Toulouse, G., Accident risks in disturbance recovery in an automated batch-production system, Human Factors and Ergonomics in Manufacturing, Vol. 12 (4) 383-406, 2002.

Vautrin, J.P. & Dei-Svaldi, D., Work accidents in automated plants: Evaluating a preventive model. Paris, France: INRS, 1989.