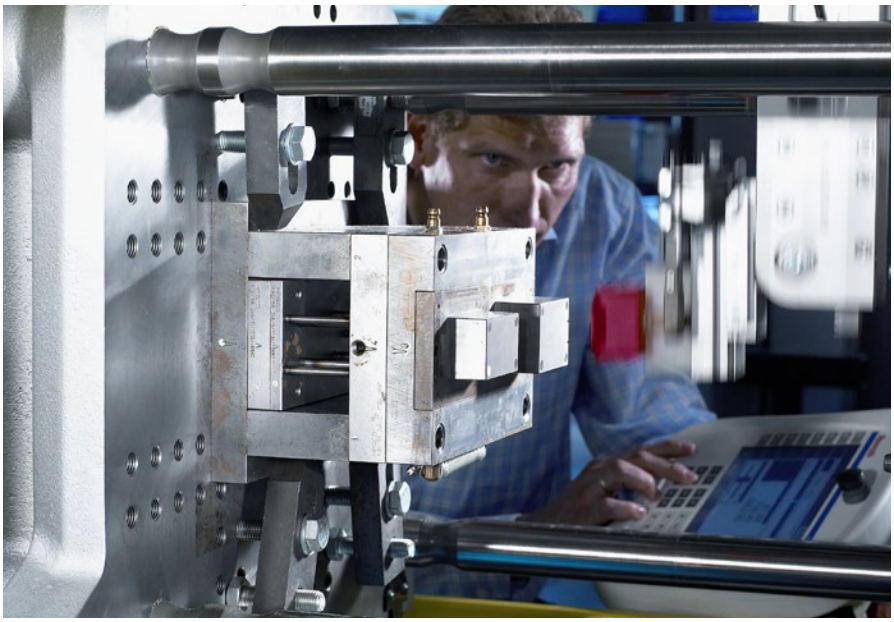
Drive & Control
profile

# Safety from a systems integrator perspective



With lab equipment that's properly designed and application-optimized from the beginning, it's possible to achieve substantial energy savings.

*By Gary Thrall, Senior Product Support Engineer, Bosch Rexroth Corp.*

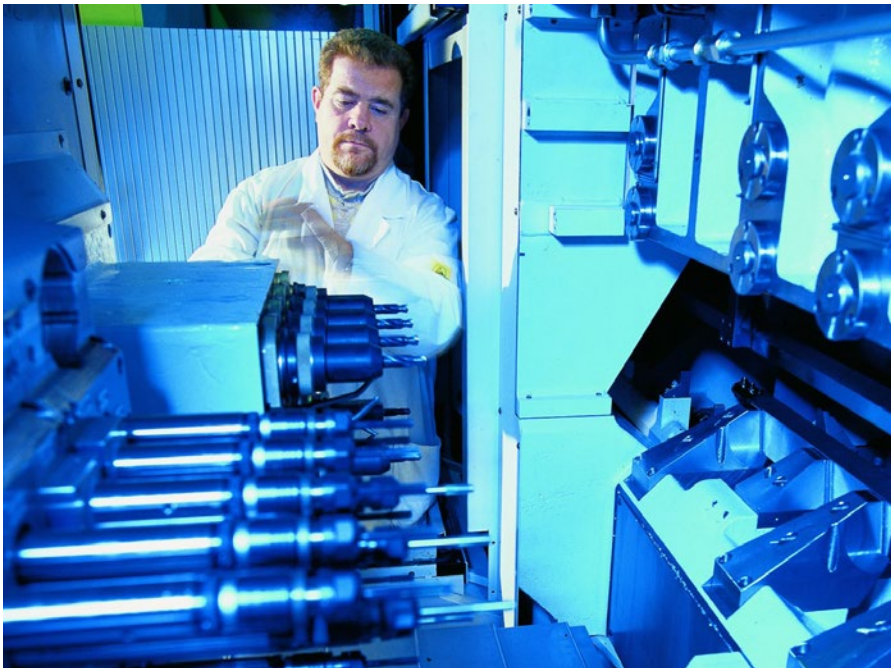
For system integrators with motion expertise, one of the most common requests is to retrofit servo controlled motion to an existing machine or process. Servo control may bring advantages of greater speed to provide reduced cycle time, faster changeover for different product variants, or a move profile that avoids existing mechanical problems. Modifying existing or adding new motion requires consideration of the functional safety of the machine.

**Functional Safety**

Functional safety is the part of a machine or safety equipment that depends on the proper operation in response to its inputs, including safe response to equipment failure and operator errors. Its purpose is to provide a workplace that is free of unacceptable risk of injury to personnel or damage (direct physical damage to the equipment or product in process or indirect damage like loss of productivity, environmental

## Overall Steps to Applying Safety

- Determine the limits of the machinery
- Identify hazards through individual hazard analysis or task-based analysis
- Evaluate the risk, and determine if it has been adequately reduced
- After each step in the process, it is also important to evaluate if new hazards have been created.
- The hazard evaluation process is then repeated with successive iterations until all identified risks have been mitigated.
- Human factors must be considered, especially in retrofits, where the process that an operator executes is being changed. It is far better to design, in advance, the special modes of access and motion required to clear jams, perform cleaning operations, etc., to ensure that added protection does not make the operator's job more difficult.



By using a standard (non-safety) input with no redundancy or diagnostics, it is possible that a single failure could cause loss of the stopping function and allow rapid motion toward the operator's hands.

hazard, or financial impact of medical and litigation costs). Functional safety is best applied from the ground up as part of the overall machine design process rather than as an add-on at the end. The conventional "frosting on top the cake" approach of considering safety as the last step may have worked to a degree when the safety approach was hard guarding and fencing. Functional safety must be designed in as part of the control system.

The Electrical, Electronic, and Programmable Systems (E/E/PS) of a machine or process control and monitor the operation, but the safety depends on proper function of the entire system. Even non-electric sources of motion, or potentially hazardous stored energy like hydraulic or pneumatic systems under pressure, or suspended weights that may fall under the effect of gravity must be included in the functional safety analysis. The functional safety is an integral part of the system—not simply a guard to prevent personnel from reaching into hazard areas unless the power is removed from the equipment.

**Retrofit Considerations**

When implemented as a retrofit, the hard part is often to convince the owner of the equipment that safety-rated components and methods are actually required. According to Controls Integrator Steve Cortese of Automation Works in Mount Prospect, IL, when an existing user has not had an accident or a runaway with only normal machine controls, he may not see the need for redundant safety-related control architecture. When past practice was to open a guard door and engage a setup bypass circuit that allows normal jogging, he may not see the need for monitored, safely-limited speed to ensure that a single failure cannot result in unexpected or uncontrolled motion—putting the machine operator into danger.

As another example, a high production automotive airbag assembly manufacturer described its method of improving cycle time by connecting a light curtain at the access to the load/unload station to the forward overtravel limit input of the servo drive that moves the bag folding arms. If the operator reaches in while the machine is still moving toward the unload station, the axis would stop; if moving away after releasing the completed airbag, motion would be allowed even though the operator's hands were through the curtain. By using a standard (non-safety) input with no redundancy or diagnostics, it is possible that a single failure could cause loss of the stopping function and allow rapid motion toward the operator's hands—the hazard they were attempting to avoid. Overtravel input is a circuit in the drive designed with normal good practice that had never failed to a hazardous condition—yet. This is the place for the Safe Direction drive feature as defined in IEC EN 61800-5-2.

In retrofits, the original system may not be up-to-date on the basic

guarding and interlocking using the conventional methods of removing power when doors are open, to prevent unexpected motion that may present a risk to personnel. Often a simple, single-channel, non-redundant emergency stop to remove power is all that was provided. Adding the proper guarding and door interlocking that drops power to servo drives may result in new errors and sequence restart issues. Dropping input power contactors also puts stress on servo drives' bus capacitors, wastes energy from discharging and recharging, and takes time to restart that could be used for the production cycle.

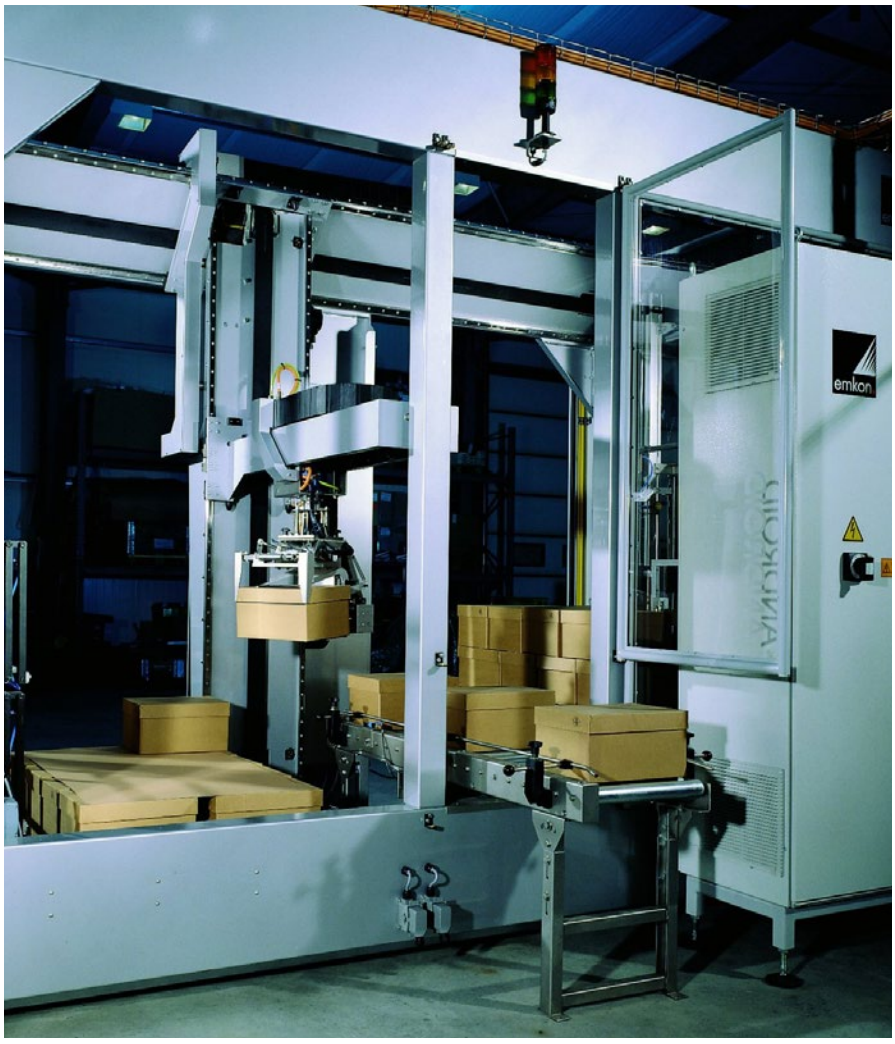
A tip from Controls Integrator Dave Stuber of Custom Controls Solutions (www.ccs-motion.com) in St. Charles, IL, is to use the Safe Stop 2 functionality, as defined in standard IEC EN 61800-5-2, which allows the drive to maintain torque and hold position while stopped. All axes in a complicated system can maintain position and synchronization while doors are opened for setup adjustments. The safety function monitors for motion and shuts down to no torque if there is motion beyond a determined safe limit. Power cycling stress, contactor wear, time delay, errors and additional logic for mid-cycle restart are avoided. These new techniques are allowed under changes to standards like NFPA 79-2007, permitting a servo drive designed for the purpose to be used for stop functions without requiring power disconnect by an electromechanical device.

**Safety Design Procedure**

The overall steps to applying safety are the basis of most standards today. First, determine the limits of the machinery, then identify hazards through individual hazard analysis or task-based analysis, estimate the risk, evaluate the risk, and determine if the risk has been adequately reduced. If unacceptable level of risk still exists, proceed with the risk reduction for that hazard.

The priority for risk reduction is to first remove the risk by inherent design or change in the process (move the column where an operator might be crushed if struck by a moving machine). If not possible, then add safeguards (e.g., create a mechanical barrier to keep the operator out of the area and automatically reduce the speed of motion if he must enter and still move the machine for recovery/

**Functional safety is the part of a machine or safety equipment that depends on the proper operation in response to its inputs, including safe response to equipment failure and operator errors.**



jam removal operations). For any residual risks, provide information for equipment use so the operator can avoid the remaining hazards. If the protective measure involves the safety related parts of the control system, standards define an iterative process (the “V-model”) for specification, design, coding, testing, integration and validation of the control system.

After each step, it is also important to evaluate if new hazards have been created. For example, if a mechanical guard that has been added to protect an operator from possible hand injury is positioned in a way that he can be trapped between the guard and a wall, a new hazard of fatal injury may have been created. The hazard evaluation process is then repeated with successive iterations until all identified risks have been mitigated.

Particularly in retrofits where the process that an operator executes is being changed, the human factors must be considered. Adding protection that makes it difficult or impossible for the operator to do his job will most certainly cause him to find a way to disable or work around the intended protection. It is far better to design, in advance, the special modes of access and motion required to clear jams, remove bad product, do cleaning operations, and any other tasks outside of the normal automatic cycle of the equipment; so the accepted solution does not defeat the safety measures installed to prevent injury and damage.

**Best Current Technology in Servo Drives**

It is in these special modes that the safe motion functions defined in IEC EN 61800-5-2 Adjustable speed electrical power drive systems, Safety requirements—Functional come into play. Servo drive safety functions defined in IEC EN 61800 are now offered in safety certified servo drive equipment that can allow power to remain applied and enable motion in special modes. These features include Safe Operating Stop, Safely Monitored Deceleration, Safe Maximum Speed, Safe Limited Speed, Safe Direction, Safe Limited Increment, Safely Monitored Position, Safely-Monitored Stopping Process, Safe Homing, and Safe Braking and Holding System. These drive safety solutions can easily be integrated into existing and new machines, providing acceptable levels of risk while enhancing machine productivity and making machine safety functions transparent to the machine operator.



Bosch Rexroth Corporation
14001 South Lakes Drive
Charlotte, NC 28273-6791
Telephone (800) 739-7684
www.boschrexroth-us.com