copley controls
Precision Motion Control

TECHNICAL NOTE | 2025 Rev 3 — April 2025

TECHNICAL NOTE TN003 – **FUNCTIONAL SAFETY IN MACHINES**

OVERVIEW

Functional safety is growing in importance as robots, automated vehicles and humans interact and share workspaces. This paper reviews the concept of functional safety as it relates to machinery. The design steps for a safe automated guided vehicle (AGV) are outlined and the methodology for determining appropriate PL/SIL safety ratings discussed. The most common motion control safety functions are presented. The paper concludes with a review of the system architectural implications of machine safety.

MACHINE SAFETY

There are formal steps to guide the design of a safe machine. The process is rigorous and well-documented in a range of standards including the Machinery Directive (2006/42/EC). Greater insight into the process can be gained, however, by working through an example — an AGV.

STEP 1: SPECIFICATION AND MODES OF OPERATION

First define the performance characteristics (speed, payload, etc.) and modes of operation (setup, runtime, maintenance, etc.) for the AGV. For this discussion, key parameters are:

- **AGV top speed:** 2 m/s.
- **Payload:** up to 50 Kg.
- **Potential collision response:**
  - Speed limited to 0.2 m/s, 3 m from point of impact.
  - Controlled stop 1 m from point of impact if obstacle still present.

STEP 2: HAZARD IDENTIFICATION

Next, identify hazards during all phases of the machine life cycle. Typical hazards to humans include crushing, severing of fingers, puncture wounds, burns, high audible noise, entrapment and entanglement. The primary hazards in this example are crushing and puncture wounds.

STEP 3: RISK ASSESSMENT

Risk assessment uses a range of scoring tools based on the severity of a hazard and the probability of it occurring. The tools vary by industry and region but employ the same basic techniques. The result is a quantification of original risk.

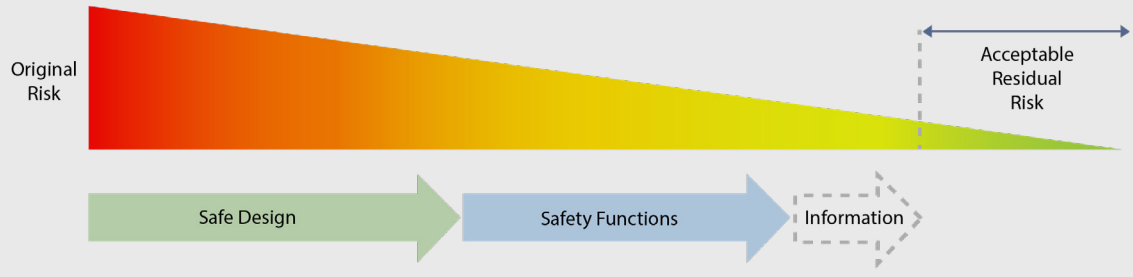

Figure 1

STEP 4: RISK REDUCTION

The final step is the reduction of original risk to acceptable residual risk. The process follows a three-level method as shown in Figure 1. The definition of acceptable residual risk varies by industry and region. Machine builders may also decide to reduce acceptable residual risk beyond the regulated level.

Level 1: Safe Design. Safe design employs inherent protective measures which may have a negative impact on machine performance. Some interpretations of the process include the use of physical guarding as part of the safe design. Safe design techniques include limiting speed (low bus voltage with appropriate motor back-EMF constant), using motors capable of very limited torque and smooth rounded surfaces.

The AGV and payload are designed to have rounded surfaces eliminating the risk of puncture wounds. The AGV is, however, capable of high speeds with a large payload resulting in high kinetic energy. The risk of crushing has not been reduced. Appropriate safety functions are therefore required.

Level 2: Safety Functions. There are a range of standard, pre-defined safety functions, which are reviewed in detail in the Safety Functions section. For this design, safe limited speed (SLS), safe stop 2 (SS2) and safe operating stop (SOS) are appropriate. SLS ensures the AGV speed is reduced in the event of a potential collision, increasing the plausibility of collision avoidance. SS2 ensures the AGV will stop before the point of impact. SOS ensures the AGV safely holds position until the obstacle has been cleared.

Level 3: Information. If the available safety functions do not reduce the risk to an acceptable level, then information — in the form of warnings and/or direction to wear protective equipment — must be posted at the operating space entrance and/or on the machine.

SAFETY FUNCTION RATING: PL AND SIL

Once the safety functions are defined, it is necessary to determine their required ratings. PL (ISO 13849-1) and SIL (IEC 62061) are two different paths to the same destination — a safety rating for a safety function. PL is machine-centric, while SIL has its origins in the process industries. IEC 62061 is a newer SIL standard focused on machine safety. But it is for electrical control systems only — pneumatics and hydraulics are excluded. In general, a safety function has both a PL and SIL rating.

To determine the required PL/SIL rating for a safety function, a risk analysis must be performed. The analysis is based on the severity of injury caused by the hazard, the exposure time to the hazard and the possibility of avoidance of the hazard if the safety function fails on demand. A typical analysis is shown in Figure 2. The path taken for the AGV SLS, SS2 and SOS functions is highlighted. The required ratings are PLd and SIL2.

Figure 2 shows the equivalence of PL and SIL ratings. There is no SIL equivalent to Pla, which is rarely applicable in motion control systems. Higher ratings (PLe and SIL3) have a lower probability of dangerous failure of the safety function per hour and consequently higher risk reduction. A higher PL/SIL rating places greater demands on system architecture, diagnostic coverage and mean time to failure (MTTF) of system components.

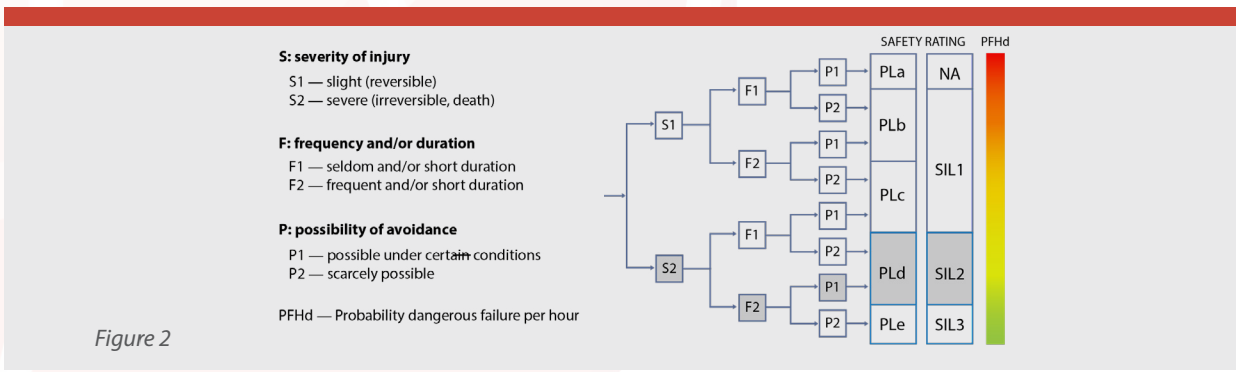

Figure 2

SAFETY FUNCTIONS

Some of the more common safety functions are outlined below.

SAFE STOPPING AND POSITION HOLDING FUNCTIONS

STO — SAFE TORQUE OFF

Function: Disables the drive power stage so the motor can generate no torque, motor coasts to a stop if moving (SS1 normally used for stopping if available).

Application: Activated by emergency stop (E-Stop), interlock (maintenance), collision detection.

Benefit: Safety contactors which physically disconnect the drive from the motor are eliminated.

SS1 — SAFE STOP 1

Function: Activates deceleration at a monitored rate, then activates STO after a configurable time. Often used in conjunction with safe brake control (SBC).

Application: Activated by emergency stop (E-Stop), collision detection.

Benefit: Same as STO but also limits coasting distance, which may reduce the size of safety buffer zones for high kinetic energy loads.

SS2 — SAFE STOP 2

Function: Motor is stopped by controlled breaking, then holds position via SOS.

Application: Activated by emergency stop (E-Stop), collision detection.

Benefit: Same as SS1, but position can be held without a brake. Downtime is potentially shorter due to uninterrupted closed loop control.

SOS — SAFE OPERATING STOP

Function: Motor holds current position within a window, falling back to STO if position is out of the window. Often used in conjunction with SS2.

Application: Activated by interlock to allow human interaction or to clear an obstacle.

Benefit: Same as SS2.

SBC — SAFE BRAKE CONTROL

Function: Supplies a safe output signal to disengage a mechanical holding brake on the motor. The brake must require a current to operate against a spring. Typically used in conjunction with STO, SS1.

Application: Activated by E-Stop or interlock when motor is at rest to allow human interaction, particularly when gravity is involved.

Benefit: Prevents damage and potential injury due to gravity.

SAFE MOTION FUNCTIONS

SLS — SAFE LIMITED SPEED

Function: Ensures that a predefined speed limit is not exceeded. Different limits depending on direction are possible. If the speed is exceeded, a configurable response is initiated. The response is typically STO as the over-speed is most likely caused by an encoder fault.

Application: Safe speed to allow human interaction and proximity.

Benefit: Higher productivity when a human is not present, elimination of guarding.

SLP — SAFE LIMITED POSITION

Function: Ensures that predefined position limits are not exceeded. If the limits are exceeded a configurable response is initiated. The response is typically STO, as the outside-limit condition is most likely caused by an encoder fault.

Application: Establishes protected zones.

Benefit: Elimination of guarding and physical limit switches.

SDI — SAFE DIRECTION

Function: Ensures that motion is in the predefined direction only. If the direction is incorrect, a configurable response, typically STO, is initiated.

Application: Allows workpieces to be removed if the machine is moving in a safe direction away from the operator.

Benefit: Productivity increase and protection of machinery that should only turn in one direction.

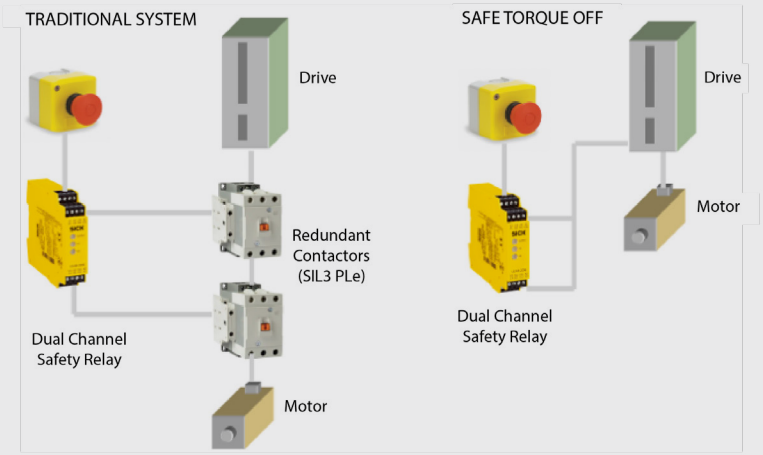

Figure 3

SAFE TORQUE OFF (STO)

STO is the critical fallback state of many safety functions and warrants further discussion. The goal of STO is to ensure that no torque is generated by the motor. Prior to STO, for a SIL3 Ple rating, redundant contactors were used to physically disconnect the drive from the motor as shown in Figure 3.

For multi-axis applications, the cost becomes prohibitive. In battery-powered mobile applications, weight and space are a factor. STO eliminates the need for contactors via discrete, redundant enable inputs for the drive power stage. It is a hardware solution with no firmware involved.

Figure 4 shows a simplified servo drive power stage. The power transistors are depicted as switches. The motor is brush-type, but the same principles apply for a brushless motor and full six-transistor inverter. To drive current through the motor, a transistor on both the "high side" and "low side" of the bridge must be closed. Closing A and A* causes current to flow in the direction shown.

If either of the redundant enables become inactive, no current can flow in the motor. The motor is now in a safe state.

Servo drive STO implementations have different ratings depending on failure mode and effects analysis (FMEA) of the power stage and STO enable circuitry. Drive manufacturers also specify varying diagnostic requirements to achieve the desired PL/SIL rating. More advanced servo drives provide automated diagnostics performed by a safety-rated processor.

SYSTEM IMPLICATIONS OF SAFETY FUNCTIONS

In many systems, the drive has STO capability only. All other safety functions are handled by a safety PLC designed to conform to safe architecture and firmware guidelines. The safety PLC, as shown in Figure 5, performs a monitoring function via a second encoder. If a safety function is triggered, the safety PLC activates STO to disable the drive power stage.

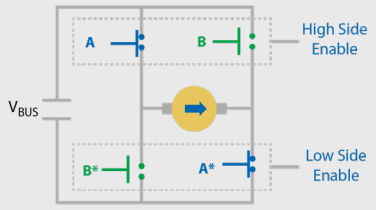

Figure 4

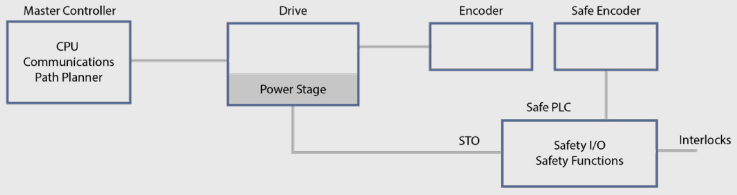

Figure 5

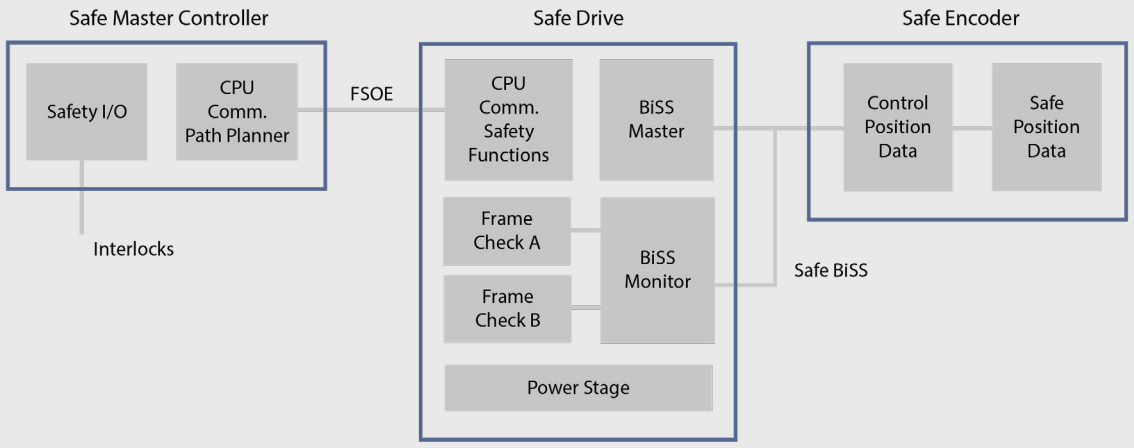

Figure 6

The current trend is to incorporate safety functions in a safe drive connected to a safe encoder. This reduces system complexity and simplifies wiring. If high safety function ratings are required, the encoder provides redundant position information (two individual readings), as shown in Figure 6. A safety-rated protocol is employed between the encoder and drive as well as redundant communication frame monitoring in the drive. The drive and encoder become a safety system. If additional diagnostics are provided by the drive, it may be possible to use a Pld/SIL2 suitable encoder for a PLe/SIL3 safety function.

STO is not connected to the drive power stage. Interlocks and collision detection sensors are connected to a safe controller which can command STO and other safety functions to multiple drives via a safety-rated communication network. In Figure 6, the safety network is EtherCAT® employing functional safety over EtherCAT® (FSOE).

CONCLUSION

Functional safety is a growing trend. Its goal is to reduce the risk that remains after safe design measures to an acceptable level. For machinery in the motion control industry, this is accomplished by a standard set of safety functions. These are rated by PL or SIL methodologies which consider hazard severity, frequency of exposure and possibility of avoidance. The result can be simplified, lower-cost systems, increased productivity and safer machine-human interaction without the need for bulky protective equipment.

copley controls
Precision Motion Control

FOR MORE INFORMATION

Visit us at www.copleycontrols.com
(781) 828-8090