From Risk to Requirement

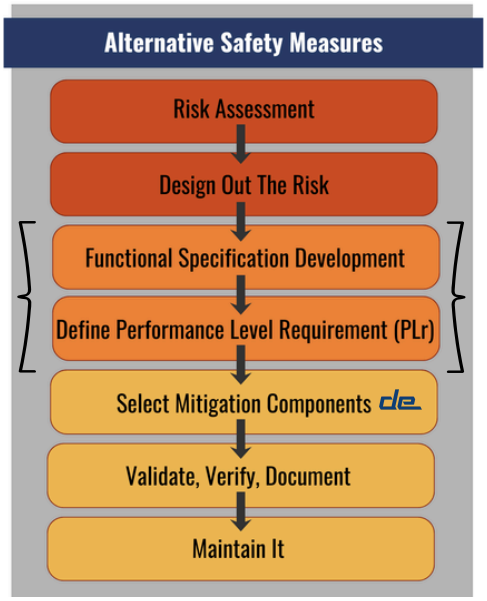
How to define what your safety system must do and how well it must do it.

Last month, we covered *Risk Assessment* and *Designing Out the Risk*, identifying hazards, who is exposed, and how to eliminate or reduce risk at the source.

This month, we take the next step and answer two questions that must be resolved before any components are selected:

> *What exactly must the machine do when a hazard is detected?*
> *How safely does the machine need to react?*

That's where *Functional Specification Development* & *Performance Level Requirement (PLr)* comes in.



Without them, you're not engineering a safety system. You're just selecting parts and hoping they solve the problem.

PART 1

Functional Specification Development

A functional specification is the blueprint for your safety system. It defines the required behavior of the machine before a single component is chosen. Think of it as the bridge between your risk assessment and your engineering design.

The risk assessment tells us what the problem is. The functional specification takes that information and answers a different question:

> *What safety functions are required, and how must they perform to reduce risk?*

Just as importantly, a functional specification establishes the boundaries of safe operation.

> *A machine may be engineered and validated to safely perform one task, but that doesn't automatically mean it's safe for another.* ***The safety functions were designed around specific hazards, specific operator interactions, and specific operating conditions. Change those considered details, and the risk can change as well.***

This is why the functional specification is so important. It documents the required safety functions, the conditions under which they must operate, and the hazards they are intended to address, creating a clear roadmap for safety system design.

When a machine is used outside those assumptions, the original safety functions may no longer provide the intended level of protection because they were designed and validated for a different set of tasks and associated risks.

To illustrate, consider a machine with a guarded access door. The risk assessment identifies hazardous motion inside. A functional specification for that scenario defines behavior:

Condition	Required Machine Behavior
Normal operation	Machine runs automatically; guard door remains closed
Guard door opens	Hazardous motion stops; stored energy is removed or properly constrained; restart is prevented
Resuming operation	Door must be closed; operator performs manual reset; deliberate restart command is given

Why this matters:
A machine isn't safe because it has safety components. It's safe because the right safety functions were defined for the job it's expected to perform.

Notice that nothing above specifies a component. A well-written functional specification removes assumptions and creates a shared roadmap for everyone involved (safety engineers, controls engineers, and machine operators).

Common safety functions that appear during this process include: **emergency stop, safe stop, guard door monitoring, prevention of unexpected startup, manual reset, restart interlock, safe speed monitoring, energy isolation, safe exhaust, and safe load holding**. The applicable functions are determined by the hazards identified in your risk assessment.

PART 2

Defining Performance Level Required (PLr)

Performance Level Required (PLr) is defined during the risk assessment, prior to any forms of risk reduction. The hazard/threat level of the machine is determined by looking at every task/hazard pair, by all who come in contact with the machine in any way.

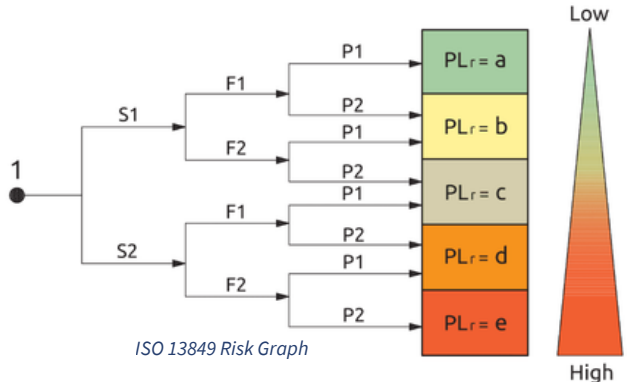
Once you know what the safety function must do, the next question is: *how safely does it need to do it?*
That's where Performance Level Required comes in.

PLr is not a rating you assign to a component. It's a requirement that the level of risk reduction a safety function must achieve. Under ISO 13849 risk graph, it's determined by evaluating three factors:

Factor	Description	Options
Severity (S)	How serious is the potential injury?	S1 — minor, reversible injury S2 — serious injury or death
Frequency (F)	How often is someone exposed?	F1 — rarely to occasionally F2 — frequently to continuously
Avoidance (P)	Can the hazard be avoided once it occurs?	P1 — possible under certain conditions P2 — difficult or nearly impossible

These factors are applied to the ISO 13849 risk graph to determine the required PLr, ranging from **a** (lowest) to **e** (highest). Severity also considers fluid power pressure and force. Whether you follow ISO or ANSI, these safety principles still apply. For detailed factor definitions and evaluation criteria, see Appendix Table A.1.

To see how different situations produce different requirements, consider two real-world examples:



ISO 13849 Risk Graph

EXAMPLE 1 — LOW EXPOSURE

A maintenance door opened a few times per year. Limited exposure duration. Hazard is visible and avoidable.

Result: PLr = c

EXAMPLE 2 — HIGH EXPOSURE

An operator reaches into a high-speed machine multiple times per shift. Serious injury is possible. Avoidance is difficult.

Result: PLr = d or e

This is why every machine must be evaluated individually. The hazards are different. The exposure is different. The required performance must reflect that.

WHY THE SEQUENCE MATTERS

Don't select components before you've done this work

One of the biggest mistakes we see is trying to select safety components before defining the safety function and PLr.
The result is often:

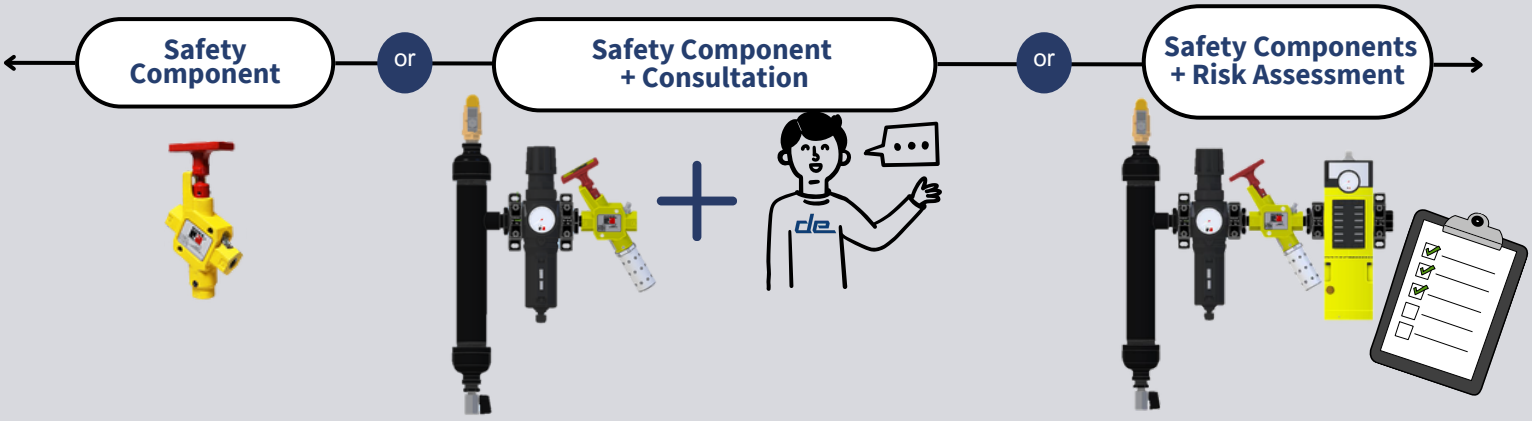
- Over-designed systems that waste money
- Under-designed systems that fail compliance requirements
- Inconsistent safety approaches across machines

When the correct process is followed, safety decisions become objective rather than opinion-based.

July 2026 Pilothouse Feature

HOW WE HELP

The Donald Engineering Difference



At Donald Engineering, we follow the ISO methodology precisely because it's structured and repeatable, giving every machine the same rigorous analysis regardless of size or complexity.

Schedule a Machine Safety Review, and we'll identify your top 2–3 risks and show you what a structured assessment looks like in your facility.

Contact our team today!

(616) 538-8340

sales@donaldengineering.com

APPENDIX

Table A.1 — Determination of parameter P based on five factors

Factor	C	B	A
1. use of the machine by		unskilled person[a]	skilled person[a]
2. speed of the part of the machine that can create a hazardous event (depending on the specific machine and time to escape from or to avoid a hazardous situation)	high speed event e.g. > 1 000 mm/s, time to hazard <1 s and/or no or too little time to escape	medium speed event e.g. 251 mm/s to 1 000 mm/s, time to hazard ≥1 s and <3 s and/or limited time to escape	low or very low speed event e.g. < 250 mm/s, time to hazard ≥ 3 s and/or enough time to escape
NOTE Any numbers in this table are purely indicative and can be different in type-C standards or based on the specific machine application. [a] 3.1.55 defines a 'skilled person' which incorporates instruction and training as well as years of practice according to this document.			
3. spatial possibility to escape from the hazard	not possible	Occasionally/rarely possible possible in < 50 % of the cases	easily possible possible in ≥ 50 % of the cases
4. possibility of recognition/awareness of the hazard (e.g. hot/cold surface, non-ionising radiation etc.)	not possible e.g. instrumentation necessary, human senses are not able to perceive the hazard, environmental conditions hide the perception	occasional/rare recognition of the hazard possible in < 50 % of the cases	easy recognition of the hazard possible in ≥ 50 % of the cases
5. complexity of the operations (human interaction in terms of numbers of operation and/or timing available for this operations)		medium to high complexity e.g. troubleshooting, use hold-to-run control to setup a part of the machine	low complexity e.g. adjust the workpiece clamps, or very low complexity / or no interaction e.g. put a workpiece into the machine
NOTE Any numbers in this table are purely indicative and can be different in type-C standards or based on the specific machine application. [a] 3.1.55 defines a 'skilled person' which incorporates instruction and training as well as years of practice according to this document.			

Image sourced from the ISO 13849-1 Manual