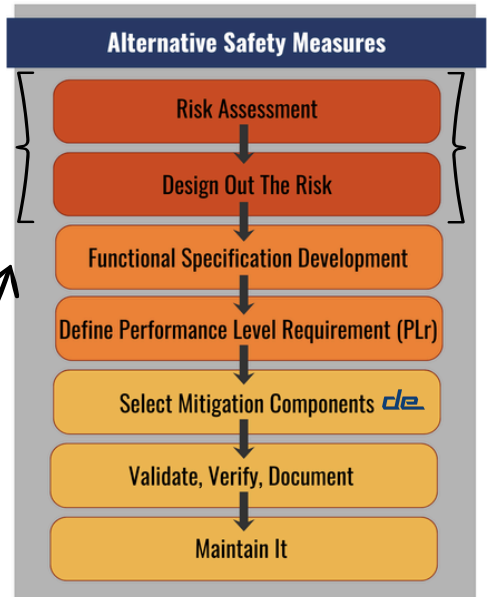
You Can't Engineer Your Way Out of a Risk You Haven't Defined.

Most companies skip straight to the solution. But the solution is only as good as the problem it was built to solve.

Last month, we introduced the idea that machine safety isn't a checklist, it's a system. We also showed how full Lockout/Tagout (LOTO) is the baseline, while engineered alternatives are often necessary to keep production running efficiently as well as safely.

That process starts with two critical steps many facilities rush through or skip entirely:

> Risk Assessment & Design Out The Risk



They are the foundation on which everything else is built. Get them wrong or skip them, and every safety device, every light curtain, every safety PLC you install is just an **expensive guess.**

THE PROBLEM

Most Safety Fixes Are Solutions Without a Problem Statement

One of the most common questions we hear is:

> *"What do I need to buy to make this machine safe?"*

When a near-miss happens, the instinct is to act fast. Add a guard. Put up a sign. Retrain the operator. And that instinct **isn't wrong, but it is incomplete**.

The problem is that the fix gets applied before the risk is truly understood.

What injury could actually occur? How severe would it be? How often is someone exposed? Could they get out of the way in time? Without answering those questions first, you're not solving the problem; you're flying blind.

The real question is:

> **"***What is the actual risk, and can it be removed before we even think about protecting from it?*

That's where risk assessment comes in. Before selecting safety devices, the real hazard, interaction, and exposure first need to be clearly understood.

STEP 1

Risk Assessment Isn't a Form. It's a Process.

A risk assessment done right is a structured analysis of every point where a person interacts with a machine and what could go wrong at each one.

ISO 12100 vs. ANSI B11: Two Standards, One Goal
Two frameworks govern how machine risk assessment is structured:

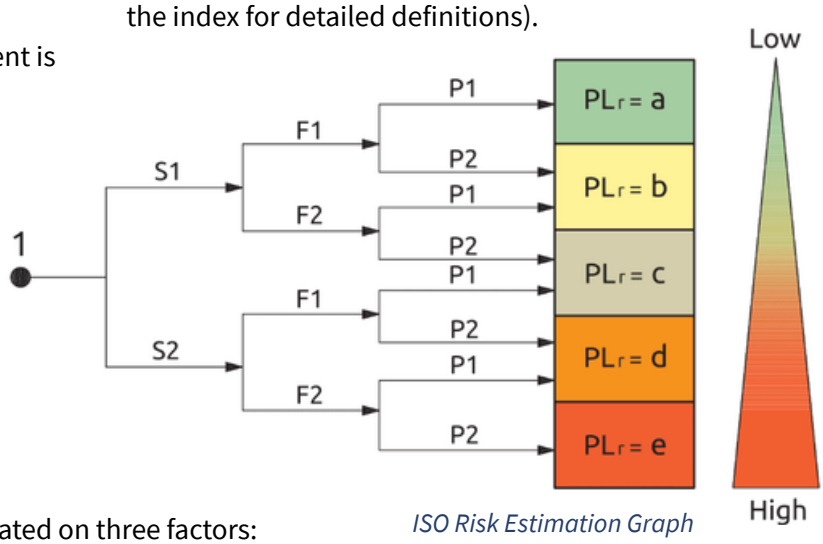
- ISO 12100 (international standard)
- ANSI B11 (US-based standard)

Both are valid, and at Donald Engineering, we are capable of working within either. In practice, we primarily follow the ISO 12100 process because it emphasizes structured hazard identification, task-specific interaction, and risk reduction before safeguards are applied.

Under ISO 12100, Each task-and-hazard pair is evaluated on three factors:

- **Severity:** How bad is the outcome? A laceration is different from a crush injury or amputation.
- **Frequency of Exposure:** How often is someone near that hazard? Once a shift? Every cycle?
- **Possibility of Avoidance:** If the hazard activates, can the person get out of the way? Or is the motion faster than human reaction time?

These three parameters feed directly into the ISO Risk Estimation Graph. A structured decision tree that determines the **Required Performance Level (PLr)**, the minimum reliability standard any safety measure must meet for that specific hazard. (Reference Table A.1. in the index for detailed definitions).



ISO Risk Estimation Graph

Key Principle
Risk assessment must be **task-specific**, not machine-specific. The same machine can have five different risk levels depending on who is interacting with it, when, and why. All this influences the final decision on what measures or processes will ultimately be undertaken.

STEP 2

Design Out the Risk Before You Guard Against It

Before selecting any component, the first question must be: *Can we eliminate this risk entirely?*

Designing out the risk means changing the machine, the process, or the task so the hazard no longer exists or no longer requires human exposure. It is the highest level of protection in the ISO 12100 safety hierarchy, and almost always the most overlooked.

What does 'design out' look like in practice?

- Repositioning a lubrication point so maintenance is performed outside the hazard zone
- Automating a manual load/unload task that required reaching near a moving component
- Redesigning a tooling changeover to eliminate the need to open a guarded area
- Moving an adjustment point so it's accessible without entering the machine's operating space

None of these solutions involves a safety device. They involve asking a better question earlier: *Why does someone need to be here at all?* When you design out the exposure, the risk isn't managed or mitigated; **it's gone.**

WHY THE ORDER MATTERS

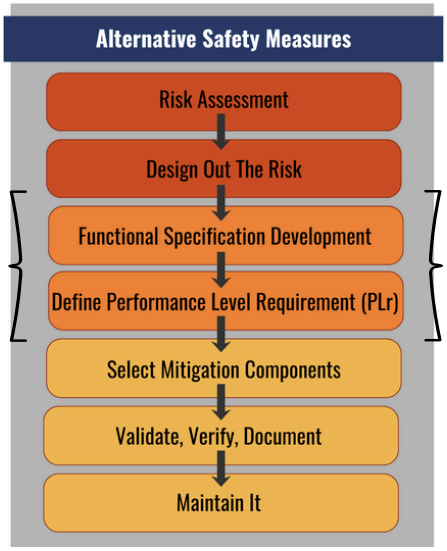
The Hierarchy Isn't Arbitrary. It's the Sequence.

A risk assessment done right is a structured analysis of every point where a person interacts with a machine and what could go wrong at each one.

If you skip risk assessment...	You don't know what PLr your safety measure must meet. A component rated for low risk may be installed on a high-severity hazard.
If you skip design out...	You can add cost, complexity, and maintenance burden to a problem that may have had a simpler solution.
If you do both first...	Every component selected has a defined purpose, a known performance requirement, and a traceable rationale.

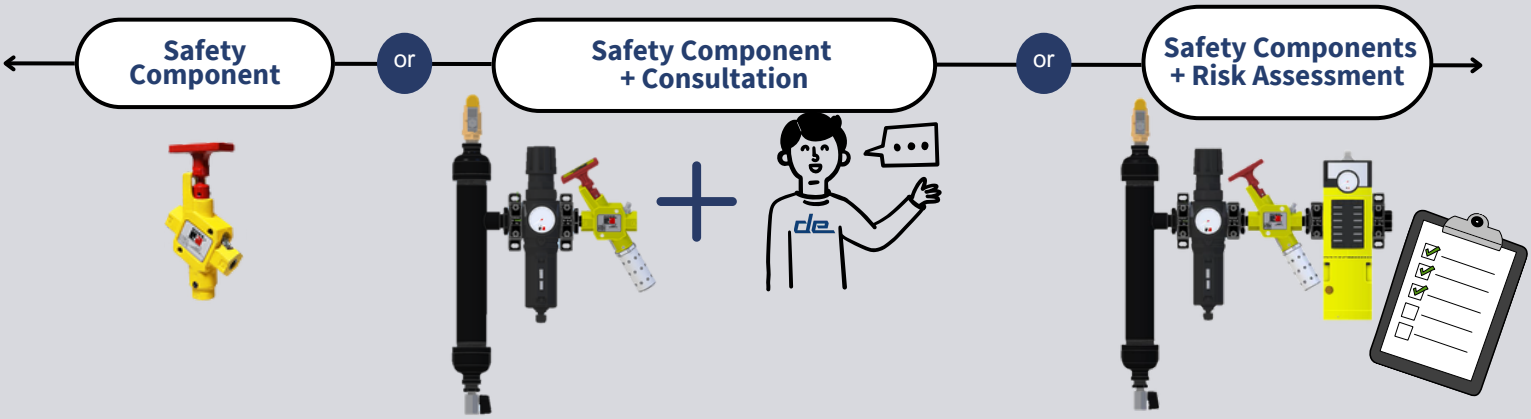
WHAT COMES NEXT

The steps that follow are only valid if these two are done first.



HOW WE HELP

The Donald Engineering Difference



We start with your machines, your processes, and the real interactions happening on your floor, not with a product catalog.

- Identify every task-and-hazard pair
- Facilitate a structured, task-specific risk assessment
- Ask the design-out question before anything is specified
- Document every step so the rationale is traceable
-

Because safety shouldn't slow production down… It should make it more reliable.

The goal isn't to sell you a light curtain. It's to make sure you need one before you buy one.

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

(616) 538-8340

sales@donaldengineering.com

INDEX

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

INDEX

Example of Risk Assessment Process

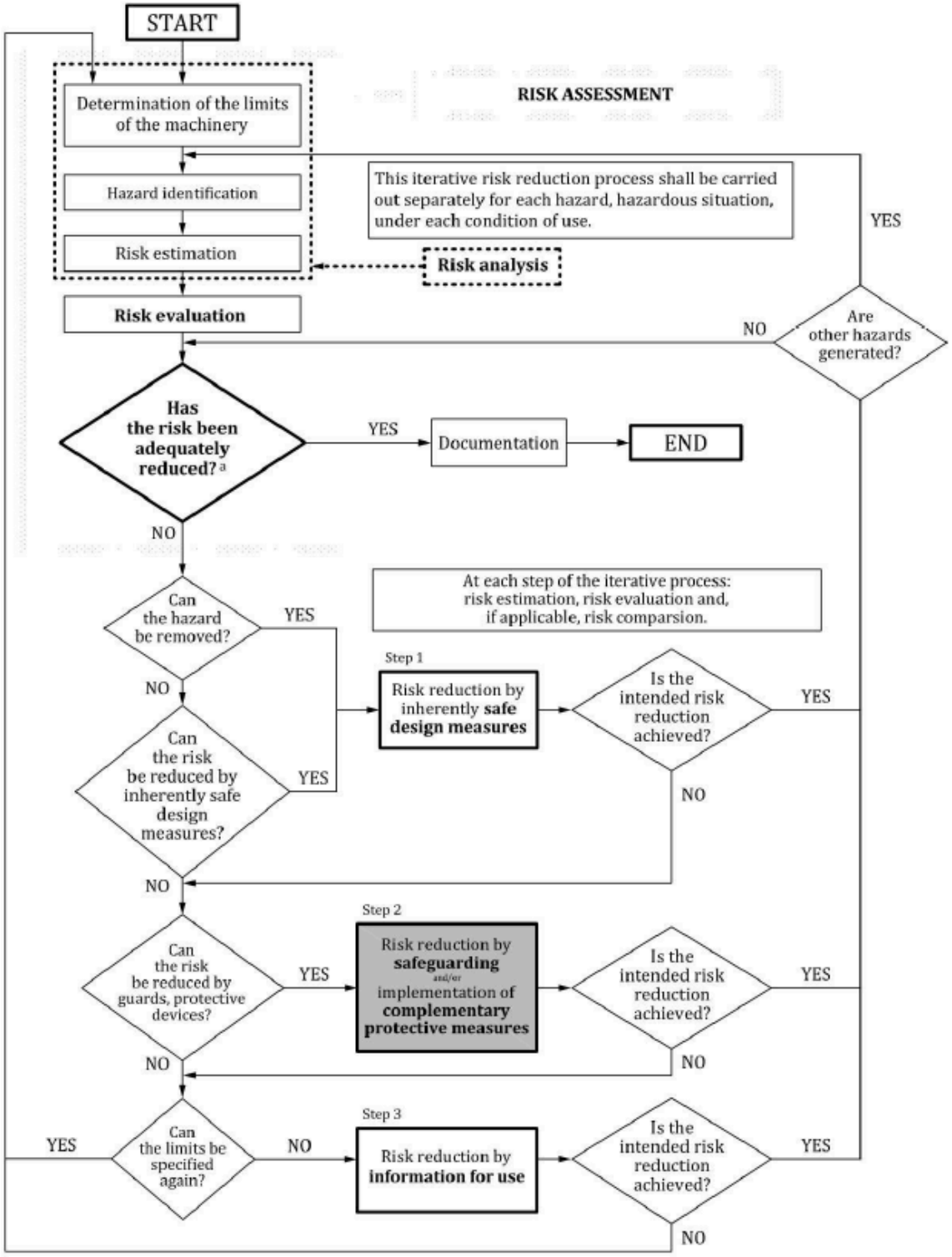


Image sourced from the ISO 13849-1 Manual