Safety FAQ – SIL, PL or Control Reliability?

We're often asked which is the "best" or "right" method of ensuring the safety related parts of a control system meet the level of reliability needed for the level of risk. The short answer, is *there's no right answer*, whatever you are most comfortable with or is mandated by your employer or customer will all lead to a safe system. However, we'll give a brief overview of them below in case you need to decide.

What is a Safety Specification?

In machinery safety there are several different ways of describing the reliability of the safety related parts of the control system (SRP/CS). The higher risk the application, the more reliable the safety system needs to be, using a safety specification defined in a standard allows this reliability to be quantified. The most commonly used specifications are Performance Levels (PL), Safety Integrity Levels (SIL) and Control Reliability.

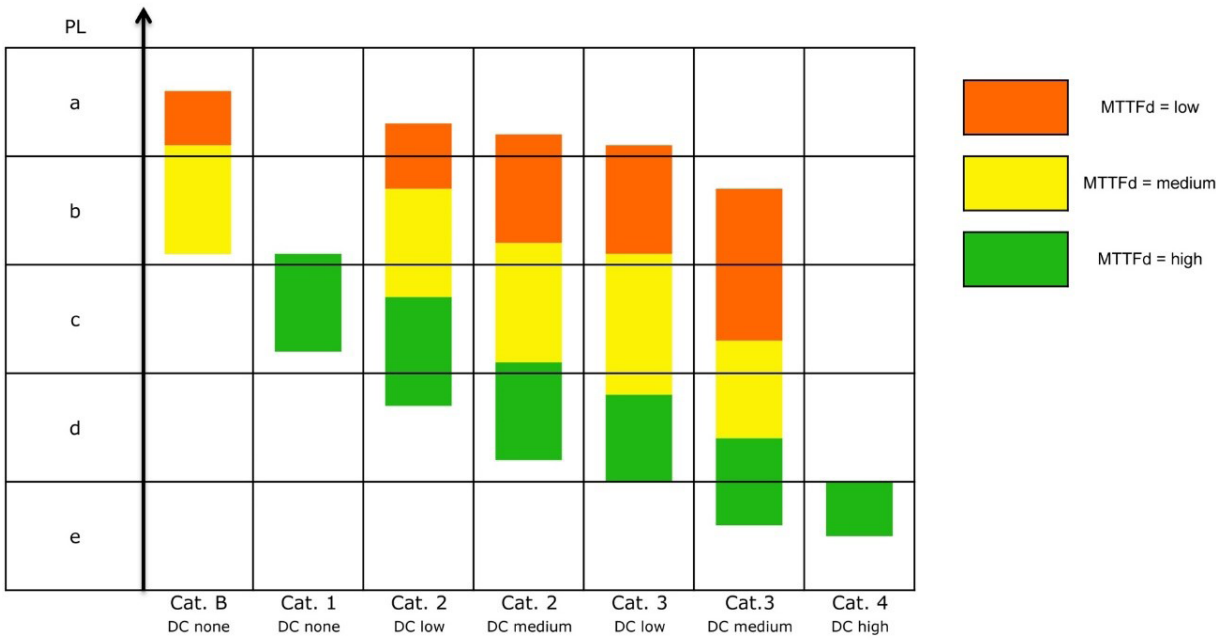
Performance Level (PL)

PLs are covered in ISO 13849-1 and apply to all safety related parts of control systems "regardless of the type of technology and energy used (electrical, hydraulic, pneumatic, mechanical, etc.) for all kinds of machinery"

Performance levels run from PLa (least reliable) to PLe (most reliable, for the highest risk applications), they are based on the probability of dangerous failure per hour (PFHd) of the safety related parts of the control system (SRP/CS). You can estimate the PL of your system using a few different parameters:

MTTFd – Mean Time to Dangerous Failure – how long until a dangerous failure
Category – Architecture of the system – single channel, dual channel and monitoring architectures
DC – Diagnostic Coverage – how likely are dangerous failures to be detected
CCF – Common Cause Failure – design to avoid multiple failures due to the same cause

Combine these parameters using the chart below to give the PL of the system.



Safety Integrity Level (SIL)

SILs are from IEC 62061 which previously only focused on electrical and electronic systems but the new 2021 revision is now applicable to all safety related control systems bringing it to be much closer in scope to ISO 13849-1

Similar to PLs, SILs are based on the probability of dangerous failures per hour (PFHd). Details on the calculations and parameters needed to calculate SILs for different architectures is provided in IEC 62061, generally calculating the dangerous failure rate of each subsystem (λd)and combining with the common cause failure factor (β) and diagnostic coverage (DC) to give a PFHd value for the system.

Control Reliability (CR)

ANSI B11.26, a US national standard on functional safety, describes Control Reliability.

"The capability of the machine control system, the engineering control – devices, other control components and related interfacing to achieve a safe state in the even of a failure within their safety-related functions"

Control reliability is a more qualitative requirement of a control system stating that if there is a failure it must result in a safe state. However, if a system meets PLd or e it can be assumed to be control reliable.

Conclusion

There have been attempts to combine ISO 13849-1 and IEC 62061 into one common standard, however, these have not yet been successful. IEC 62061 was recently released to widen the scope and ISO 13849-1 is under revision, but they are not yet in total agreement.

In the meantime rest assured that both standards can offer guidance on achieving a safe system. In fact, you can compare the three specifications that we've discussed against the Probability of Dangerous Failure per hour in the following table:

PFH_D	Performance Level (PL)	Safety Integrity Level (SIL)	Control Reliable
$\geq 10^{-5}$ to $<10^{-4}$	a	None	No
$\geq 3x10^{-6}$ to $<10^{-5}$	b	1	No
$\geq 10^{-6}$ to $<3x\ 10^{-6}$	c		No
$\geq 10^{-7}$ to $<10^{-6}$	d	2	Yes
$\geq 10^{-8}$ to $<10^{-7}$	e	3	Yes