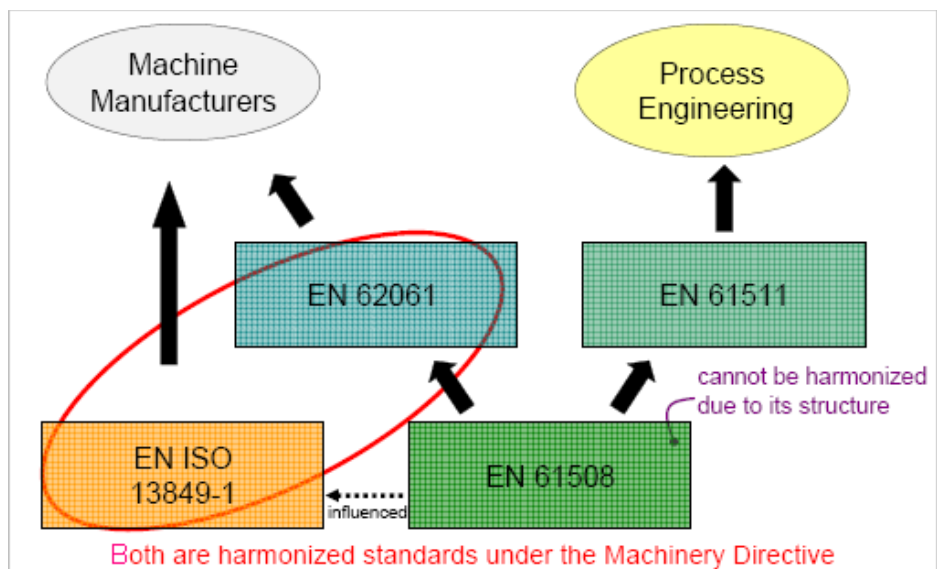


探討機械安全控制系統的功能安全標準

資料提供：台灣德國萊因技術監護顧問(股)公司

隨著功能安全的基本標準 EN 954-1 即將被 EN 62061 及 EN ISO 13849-1 所取代，機械設備的安全評估也面臨改變(圖 1)。以往，安全功能評估主要著重於安全相關的架構(迴路設計、組成元件、控制程序、安全等級)，但現在軟/硬體產品的可靠度(可能的失效)也必須透過更複雜的安全功能分級程序來加以分析。這也為機械設備的安全功能設計帶來新方向。

這類新標準已是設計安全電子裝置及軟體等最新科技時必須考量的標準。由於在設計安全相關的零件及次系統上必須從新的作法切入，使得機械的安全設計也有新的可能。此外，最新的 C-type 機械標準及新版機械指令也要求機械設備的安全設計必須經過可靠度評估。機械設備製造商在面對新的挑戰與風險的同時，也帶來了新的商機。



圖(1) — 功能安全標準：DIN EN 954-1 及替代標準

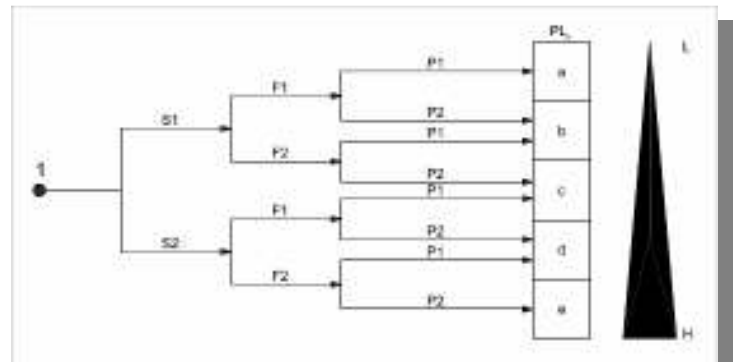
根據歐盟法令，EN 62061 與 EN ISO 13849-1 將為機械指令的調和標準，這兩項標準有著相等的法律地位。EN ISO 13849-1 適用於評估機械設備的電機安全、電子安全、可程式電子安全、機械安全、氣動安全及液壓安全；惟 EN 62061 無法使用於評估機械、氣動及液壓系統，因此與機械製造商的相關性較低。

然而，這兩項標準所規範的安全類別都適用於控制系統的安全相關部件，包括：

- 防護裝置 (例如：雙手控制裝置、互鎖裝置)、電子感測防護裝置 (例如：光柵)、壓力感測裝置；
- 控制單元 (例如：專司控制、數據處理或監控功能的邏輯單元)；
- 電力控制元件 (例如：繼電器、動力控制閥等)；以及
- 各種機械設備的安全控制系統，無論是簡單設備單元 (例如：電動工具、自動(閘)門) 或是較複雜的製程設備 (例如：包裝設備、印刷設備、沖壓設備)

上述兩項標準都是透過風險圖表來進行風險評估，但是 EN 62061 的評估結果為 SIL (Safety Integrity Level, 安全完整性等級)，EN 13849-1 的評估結果為 PL (Performance Level, 性能等級)(圖 2)。

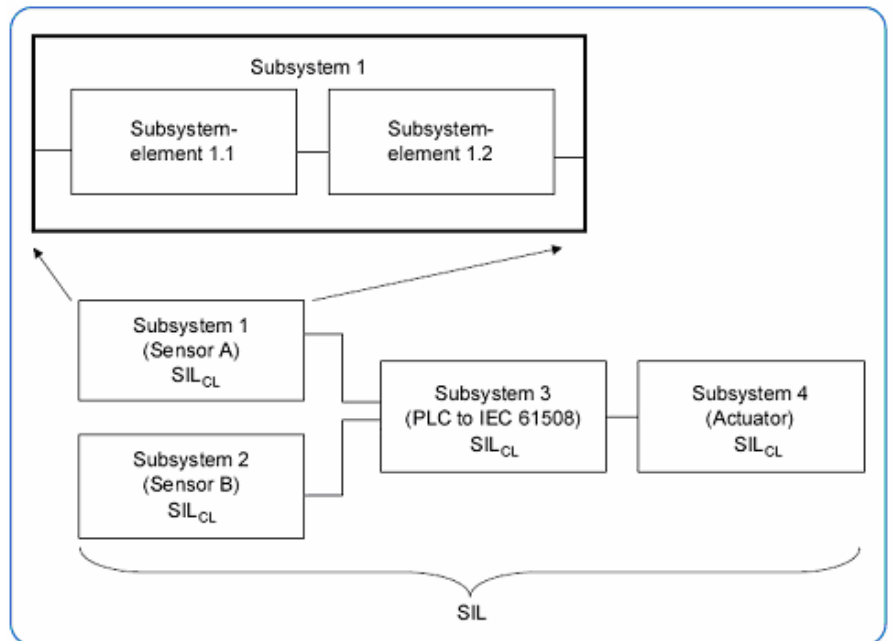
風險評估的下一步，就是將已確認的風險等級對照已採用的風險降低措施。每個已確認的風險都必須搭配一或多項，足以消除或有效降低風險的措施。接下來，就是評估安全控制系統的架構(圖 3)，並透過統計數據加以分析評估。



圖(2) — 決定安全功能的性能等級的風險圖表

前述的兩項新標準以及新版機械指令，將使得機械設備及零部件的符合性證明文件準備更具挑戰性。現有的安全控制設計必須重新評估。台灣德國萊因建議廠商宜及早了解相關要求以為將來作好準備。

如您對以上內容有任何疑問，歡迎洽詢台灣德國萊因。



圖(3) — 安全控制系統的 SIL 結構概念：次系統的等級取決於所組成的零部件，同理，系統的等級應由所組成的次系統來決定