# CE 產品安全認證

## 機械指令驗證輔導　工業機械安全相關控制系統的設計與 EN ISO 13849

K. J. CERTIFICATION CO. LTD.
坤展國際安全驗證有限公司

林建廷 BRIAN LIN

2013/7/18

坤展國際安全驗證有限公司
K. J. Certification Co. Ltd.
432 台中市大肚區遊園路二段 43 號 1 樓
Tel : +886-4-26910213 Fax :+886-4-26917117

# 工業機械安全相關控制系統的設計與 EN ISO 13849-1

歐盟新版機械指令 2006/42/EC 將於 2009 年 12 月 29 日起執行，取代現行的機械指令 98/37/EC，為因應此一新版指令，歐盟標準化組織 (CEN) 已開始標準修訂。而安全功能的基本標準 EN 954-1 亦即將被 EN ISO 13849-1 所取代，目前有許多更新版的標準已將 EN ISO13849-1 列入其中，對安全相關控制部份提出詳細的要求。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。

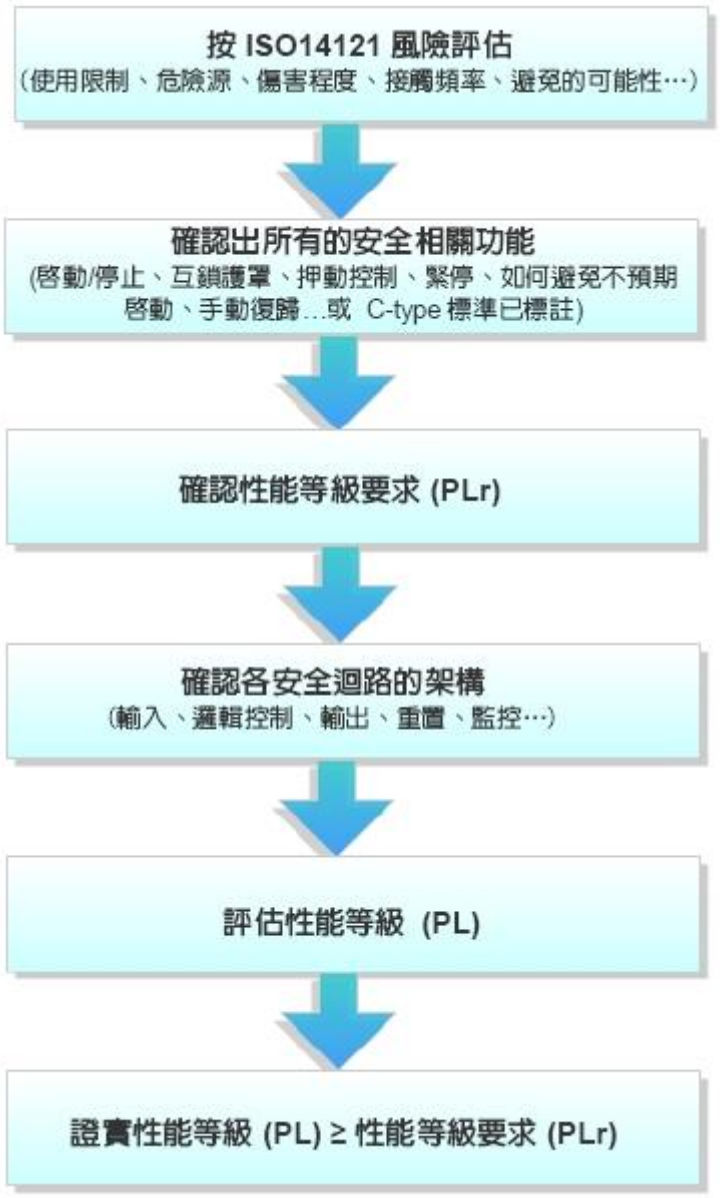
這是由於日新月異且漸趨複雜的電子相關元件所組成的系統，正逐步的被使用於各種領域，由無安全功能轉而成為具備安全功能。積體電路及微處理器等軟體元件，被採納為控制系統的核心元素，但此類元件的故障模式難以定義。因此，EN ISO13849-1 以安全等級 (safety category) 及可靠度 (reliability) 的觀點來定義機械設備安全控制系統的性能 (performance)，而非單一針對元件的故障模式。

**<Remark>**

歐盟原訂於 2009 年 12 月 31 日由新版安全標準 EN ISO13849-1 取代 EN 954-1 標準，惟鑑於許多機械製造業者尚未對新標準做好準備，歐盟因此決議延後 EN 954-1 的撤銷期限至 2012 年 12 月 31 日。

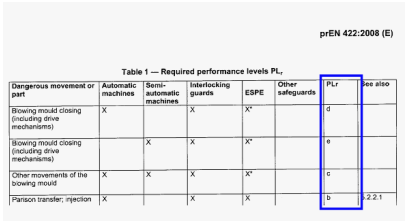
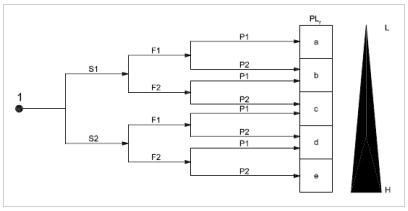
432 台中市大肚區遊園路二段 43 號 1 樓
Tel : +886-4-26910213 Fax :+886-4-26917117

- 安全相關部份控制系統的設計程序：



432 台中市大肚區遊園路二段 43 號 1 樓
Tel : +886-4-26910213 Fax :+886-4-26917117

❑ 如何確認“性能等級要求(PLr)”& 如何評估“性能等級(PL)”

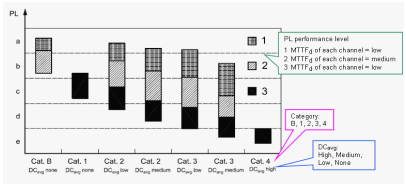
| 如何確認“性能等級要求(PLr)” | |
|---|---|
| 由 C 類標準中所標註 | 依照 EN ISO 13849-1 由風險曲線得知 |
|  |  |
| (表 1) | (表 2) |

prEN 422:2008 (E)

Table 1 — Required performance levels $PL_r$

| Dangerous movement or part | Automatic machines | Semi-automatic machines | Interlocking guards | ESPE | Other safeguards | $PL_r$ | See also |
|---|---|---|---|---|---|---|---|
| Blowing mould closing (including drive mechanisms) | X | | X | X* | | d | |
| Blowing mould closing (including drive mechanisms) | | X | X | X* | | e | |
| Other movements of the blowing mould | X | X | X | X* | | c | |
| Parison transfer; injection | X | | X | X | | b | 4.2.2.1 |




| 如何評估“性能等級(PL)” | |
|---|---|
| 評估 PL 的四個變數 | 藉由組合 4 個變數可從下表中決定出 PL |
| ▓ 硬體迴路構造<br>(種類 B, 1, 2, 3, 4)<br>▓ 元件的壽命<br>(危險故障平均時間 MTTFd-高/中/低)<br>▓ 系統的偵測能力<br>(診斷範圍 DVavg - 高/中/低/無)<br>▓ 設計的可靠性<br>(共因失效 CCF>65,共因失效 CCF<65) |  |
| | (表 3) |



前述的新標準以及新版機械指令，將使得機械設備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。

432 台中市大肚區遊園路二段 43 號 1 樓
Tel : +886-4-26910213 Fax :+886-4-26917117

## ❑ 導言

EN 13849 屬於 TYPE-B1 標準，若有 TYPE-C 標準適用，則仍以 TYPE-C 標準為準。

當控制元件被設計為提供安全功能時，此元件被稱為 SRP/CS (Safety-related parts of control system)。除此之外 SRP/CS 亦可提供操作功能，如雙手控制開關。

SRP/CS 依在可預測的狀況下提供安全功能的能力區分為五級稱為安全功能等級 (Performance level/PL). 此層級依每小時危險失效的機率(Probability of dangerous failure per hour)來定義。

| Probability of a dangerous failure per hour [1/h] | PL EN ISO 13849-1 Performance Level | SIL EN IEC 62061 Safety Integrity Level |
|---|---|---|
| $10^{-5} < PFH < 10^{-4}$ | a | no corresponding level |
| $3x10^{-6} < PFH < 10^{-5}$ | b | 1 |
| $10^{-6} < PFH < 3 \cdot 10^{-6}$ | c | 1 |
| $10^{-7} < PFH < 10^{-6}$ | d | 2 |
| $10^{-8} < PFH < 10^{-7}$ | e | 3 |

此危險失效的機率主要由幾項因子決定，包含硬體和軟體架構、失效偵測機構的能力範圍 (Diagnostic coverage/DC)、元件的可靠度(Mean time to dangerous failure/MTTFd)、一般失效原因(Common cause failure/CCF)、設計程序(Design process)、操作應力(Operating stess)、環境條件、操作程序(Operating procedures)。

432 台中市大肚區遊園路二段 43 號 1 樓
Tel : +886-4-26910213 Fax :+886-4-26917117

❑ 安全功能等級(PL)共分為五等級包含等級 B、1、2、3、4。

安全功能等級可以應用在安全相關的控制系統如:

- 保護裝置(ex. 雙手控制開關、互鎖裝置)、電子感應保護裝置(ex.光電開關)、壓力感應裝置
- 控制單元(ex. 控制功能的邏輯單元、資料處理、監控等)以及
- 動力控制元件(ex. 繼電器、閥等)

並且也適用實現各式各樣機械安全功能的控制系統 – 從簡單的機械如小型廚房機械或者自動門到產業機械如包裝機、印刷機、沖床等。

**1. 範疇**

EN ISO 13849 適用於電力/油壓/氣壓的安全控制系統

**2. 名詞解釋**

定義

safety-related part of a control system (SRP/CS)控制系統安全相關元件

控制系統的一部份，此部份對應到安全信號的輸入與產生安全相關信號的輸出

註 1: 合併的 SRP/CS 開始於安全相關輸入訊號觸發之際(包含例如: 位置開關觸動桿/滾輪)並且終止於動力控制元件的輸出.

註 2: 如果監控系統用於診斷(diagonositc)，則亦屬於 SRP/CS 一環

**3 等級區分(Specification of Categories)**

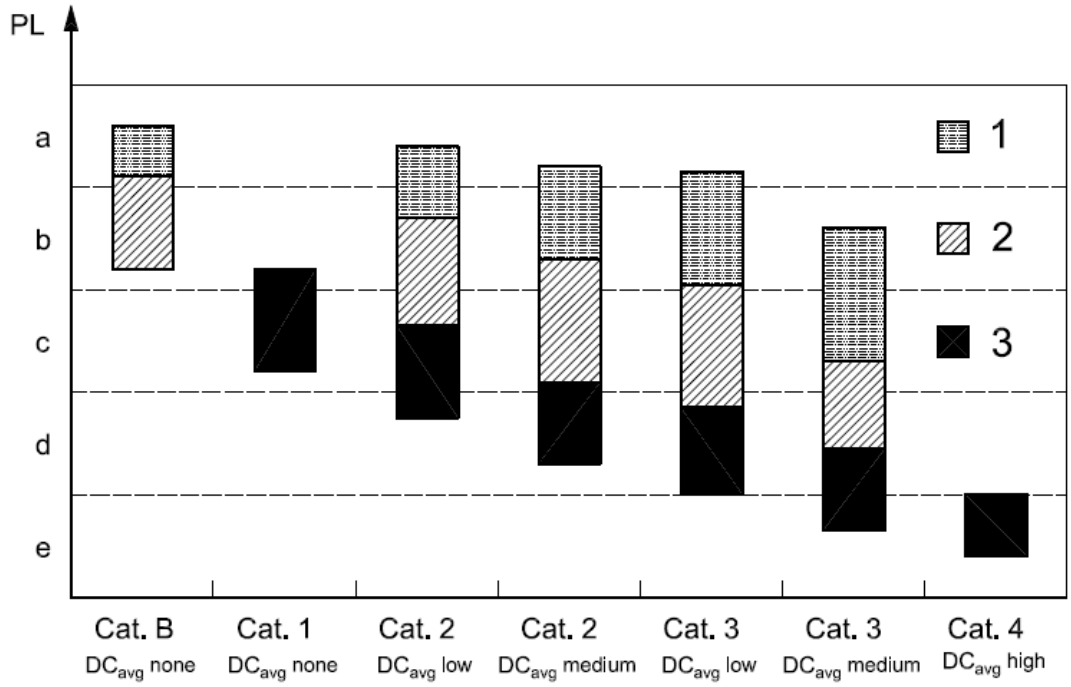
Category 等級

SRP/CS 的分類關於失效的抵抗能力(產生機率)和在失效狀況時後續出現的行為，且該行為由這些 SRP/CS 組成的架構，失效偵測能力和/或者其穩定性達成

432 台中市大肚區遊園路二段 43 號 1 樓
Tel : +886-4-26910213 Fax :+886-4-26917117

### 3.1 總則

下列的架構符合各個等級的要求。




**Key**

PL performance level

1 $MTTF_d$ of each channel = low

2 $MTTF_d$ of each channel = medium

3 $MTTF_d$ of each channel = high

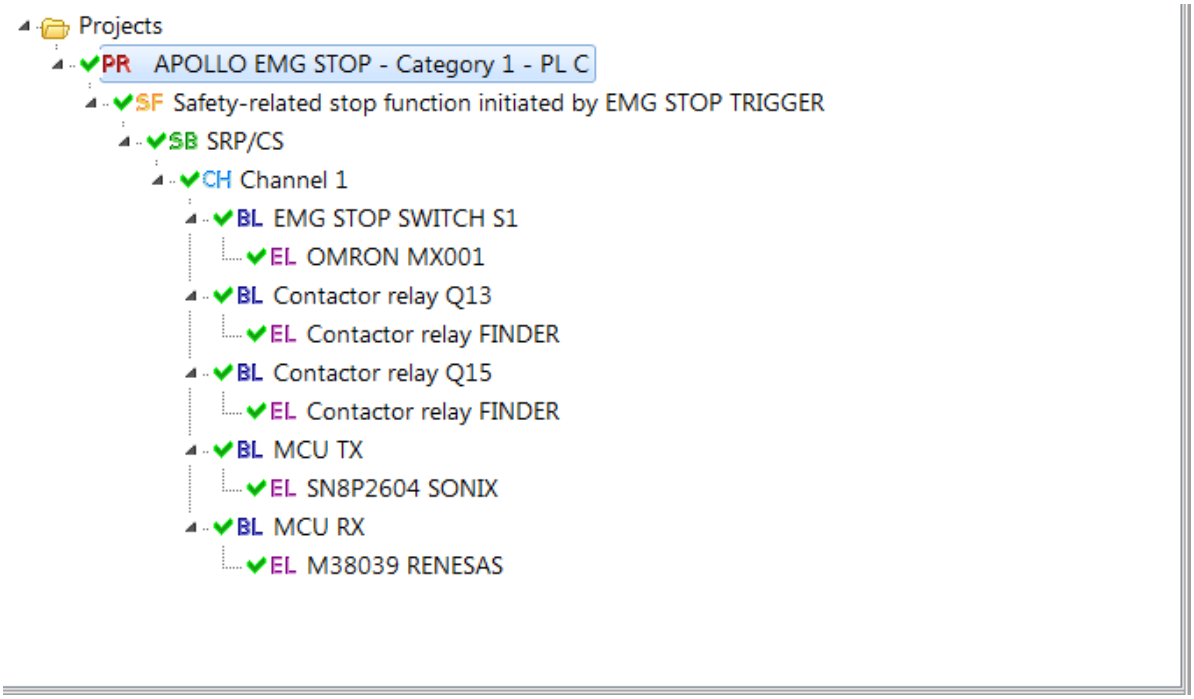
圖表表示原則性的架構與範例，任何衍伸的架構都是有可能的；但是任何的衍伸經過適當的分析工具，好讓系統可以符合 $PL_r$ 的要求。

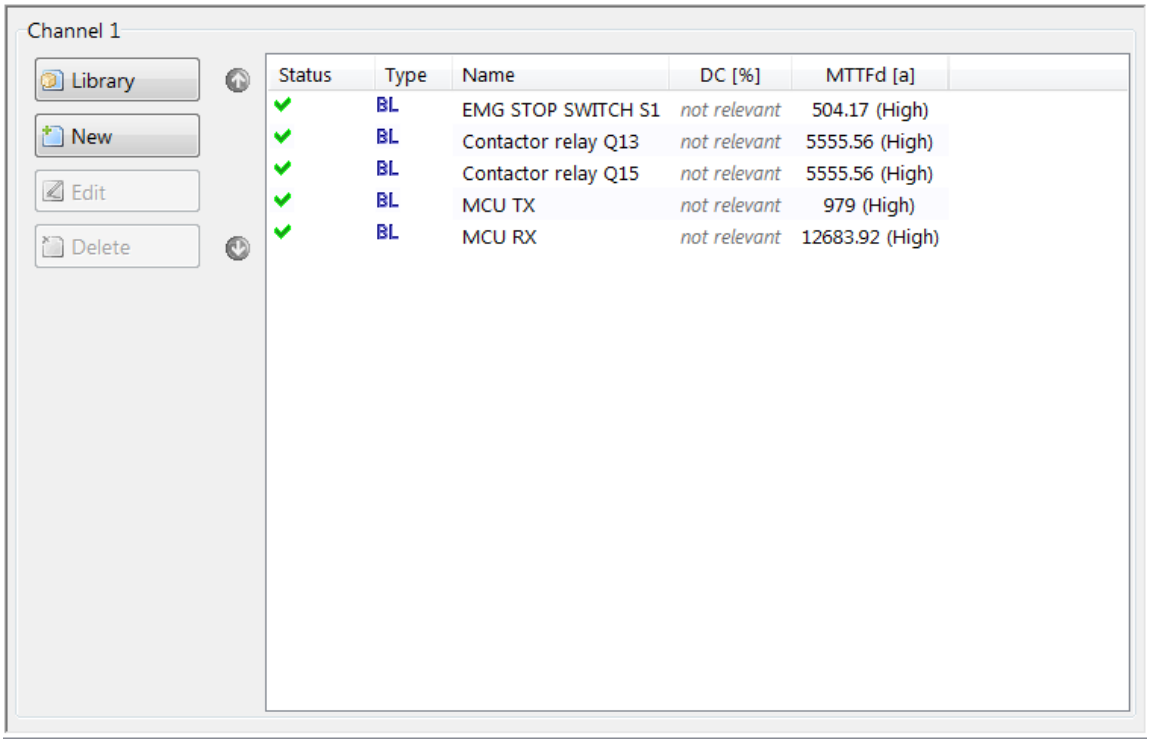
### 3.2 指令的架構

原則上大部分的機械可以找到相對應的安全等級。每一個等級都有一個安全相關方塊圖可以表示。

根據等級區分， PL(每一個通道的 MTTFd 和 DCavg)是基於指定的架構。用來評估 PL, SRP/CS 的結構必須說明如何相等於所宣告的等級。設計上如果符合各等級的要求，一般來說即等於各等級的指定的結構。

### 3.3 等級 1 (Category 1) MTTFd of each channel 高(HIGH)



坤展國際安全驗證有限公司
K. J. Certification Co. Ltd.

認證部經理
林建廷
0920-327-728

統　　編：54232837
地　　址：432台中市大肚區遊園路二段43號1樓
電　　話：+886-4-26910213
傳　　真：+886-4-26917117
E-MAIL：brian@kjisc.com
SKYPE：BRIANLIN777
網　　址：www.kjisc.com