從回授控制說起

在傳統開回路控制(open loop control)系統,我們發現輸入(下達的控制命令)與輸出結果(接受命令所要進行的動作)間可能出現誤差.而這個誤差產生的原因可能可以校正,但前提是我們要知道已經產生誤差.例如刻度盤轉一格則車速加快10 公里.但實際卻只加快 5 公里.其原因可能是被人偷改刻度錶而變成一格只加快5 公里.也可能齒輪比已被動手腳而不知.

於是在傳統開回路控制系統中,我們必須保證輸入與輸出間的關係,以保證我們給多大輸入,就可以有多少輸出.如果輸入與輸出間關係已經改變,則我們只有在某一時刻發現輸出不如預期量,才知道要調整作爲.例如我們因爲環境變化而改變了輸入與輸出的關係,則需要修改輸入量以保證獲得相同輸出量.只要輸入與輸出關係不變,則我們可正常工作直到下一次發現有問題.

所以開回路控制系統會出現輸入無法知道輸出量的真正值之現象,只好一直假設工作正常,直到有人發現輸出異常才通知進行調整.這對於需要精密控制的系統是不利的.於是我們要進行閉回路控制(close loop control)方式來確保系統精密度.

閉回路控制系統會即時把輸出的量回報給輸入端以進行驗證.如果在現有輸入量所產生的輸出量與預期量不符合,則我們可以進行相對應的動作.例如要求停機以找出原因,或調整輸入量以產生符合預期的輸出量.基本上不同的系統設計者會依據需求來進行動作.

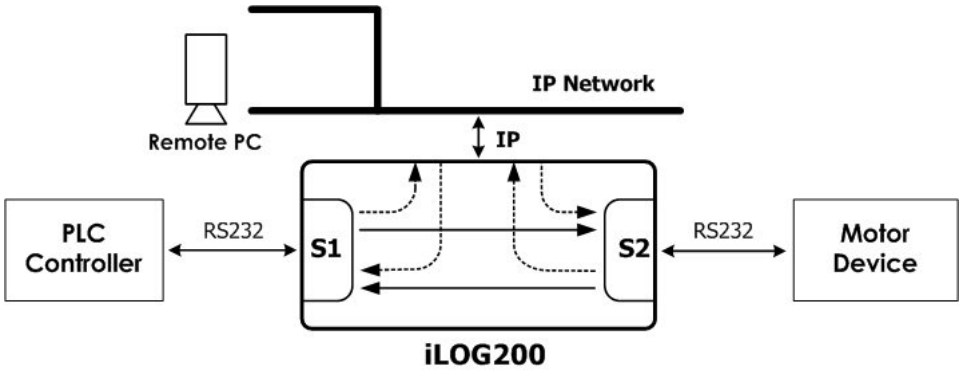
對於工廠的 PLC 控制環境中,我們通常會有一台中控電腦來下達命令給各 PLC 來執行期望動作.如果我們是開回路控制系統方式,則中控電腦只能相信底下的 PLC 會依據命令執行動作.如果操作者發現異常,則會通知中控電腦管理人員進行處理.如果我們是閉回路控制系統方式,則我們會由監控系統回報給中控電腦以判定是否動作正確.通常這是一種複雜的系統,除了增加很多成本,而且監控內容是否滿足需求都有爭議.因此除非有人員安全考慮的必要性之問題解決方案,否則成本仍是閉回路控制系統的主要考慮.

當 Stuxnet Worm 病毒出現針對 PLC 進行攻擊的過程被深入分析後,我們發現執行 STEP7 的中控電腦,在下達命令給 PLC 以調整馬達轉速時,其命令由控制程序下達之值,與真正下給 PLC 的值,已經被 Stuxnet 病毒修改,而操作人員無法知道.於是最後出現問題,卻故意引導成人員操作錯誤所造成的問題,以避免被發現是故意犯罪行爲.

由前面的說明我們知道閉回路控制系統是一個複雜的系統而不易達成.但針對

中控電腦與 PLC 間的資料傳輸監控則可以簡單的達成.亦即我們可以在中控電腦之外多加一台監控電腦..任何由中控電腦與PLC間傳輸的資料都被傳送到監控電腦.如果中控電腦操作人員設定的命令顯示,與監控電腦接收命令不同,則我們可以假設中控電腦可能有中毒而傳送被修改過的命令.

對於系統集成商而言,瑞旺科技的 iLOG200 可以監控中控電腦與 PLC 間的資料傳輸.依據要求我們可以在監控電腦準備相關軟體來處理這些資料.可以是實時顯示在畫面上與中控電腦比對.可以分析其內容如果有異常立刻報警.可以儲存以供日後分析.於是在不影響原有工作環境情況下進行類似閉回路控制系統的監控以提昇安全性.當系統出現問題時,除了傳統上中控電腦自己本身提供的資料(可能已被中毒軟體所提供)可供分析,監控電腦所記錄的資料更是一大輔助.可以加快問題的察覺及分析.



當我們由串口 1 收到 PLC 的命令後會由串口 2 轉送給馬達控制器,同時也透過網路傳給監控電腦.當我們由串口 2 收到馬達控制器的回報資料後會由串口 1 轉發給 PLC,同時也透過網路傳給監控電腦.這樣我們就可以經由監控電腦來進行安全性處理.如果有必要我們的監控電腦也可以模擬馬達控制器與PLC對話.也可以模擬 PLC 與馬達控制器對話.