如何使用主机看门狗建立可靠安全的远程监控系统

文 / Martin Hsu

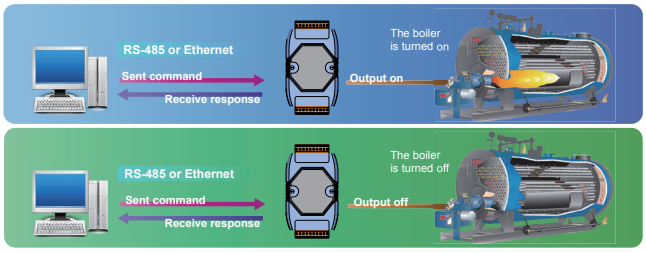
主机看门狗主要用来监控模块与主机间的运行状态。在任何一段时间内 (watchdog timeout)，若模块与主机 (PC 或 PLC) 之间无实质通讯或发生通讯问题时，模块可以做一些预防机制 (如：将预先设定的 安全值 输出等)。

远程分布式控制

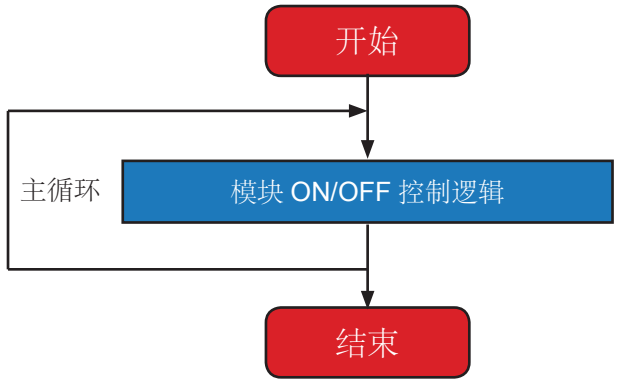
远程分布式控制的应用，实现现场运作的自动化，要如何防止自动化过程中因为通讯异常造成的意外及损失，泓格科技的远程输出控制模块均内建主机看门狗计时器及安全值的设计，让使用者可以通过这可行的运作机制，建立一套安全可靠的系统。

本文将介绍主机看门狗计时器及安全值的使用，同时辅以程序设计流程，协助用户对主机看门狗计时器及安全值的了解及如何通过程序来实现应用。

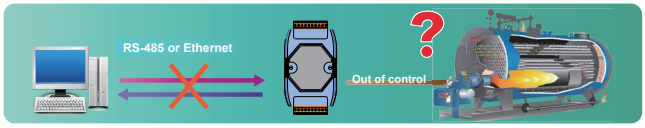
下图是展示一个简单的远程控制系统：PC 或 PLC 通过 Ethernet 或是 RS-485 网络对远程的输出模块进行 ON/OFF 控制。



这样一个简单的控制系统，程序设计上的流程如下：



上述系统，如果加热过程遇到通讯异常，例如通讯线被扯断或网络断线，控制加热的 DO 输出将无法接受控制，而系统在不受控制的情况下持续加热，这样造成的后果可能难以估计，也就是说在实际运用上不可靠，同时也有安全上的顾虑。



上图中主控端程序已经对 DO 改变输出状态，在过程中发生通讯异常时，主控端已经无法将命令发送到远程模块，这时候如何让输出模块改变输出状态？

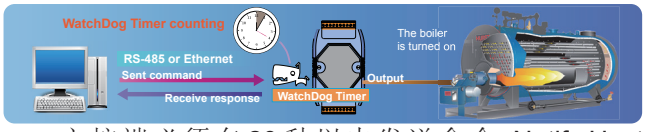
以下将以泓格 I-7000 系列及 I-87K 系列为操作模板说明在真实环境中如何使用主机看门狗搭配安全值进行设置，以及程序上必须注意的细节。

主机看门狗 Host Watchdog

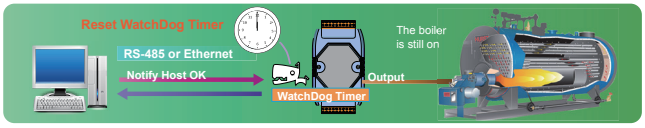
泓格科技的远程控制模块在设计时就已经有考虑到这个问题，所有依赖通讯控制的输出模块都能设定所谓的 Host Watchdog 机制，搭配安全值设置让远程分布式控制系统更安全可靠。

那什么是 Host Watchdog 机制呢？

所谓的 Host Watchdog 是主控端与远程受控模块之间通讯逾时处理机制，一开始我们必须为远程受控模块提供一个看门狗定时器 (Watchdog Timer)，并设定多久时间没有收到主控端的通知就视为逾时 (Watchdog Timeout)。当启动 WDT 定时器后，Watchdog Timer 开始计时 20 秒：

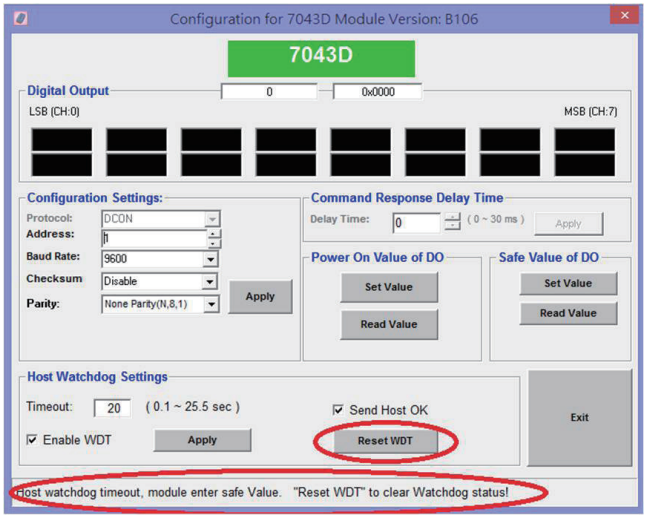


主控端必须在 20 秒以内发送命令 (Notify Host OK) 去重置 WDT 定时器 (Reset Watchdog Timer) 让定时器归零，如下图，像这样的计时机制就是 Host Watchdog 运作方式：



如果启动 Host Watchdog 后，因为通讯断线或故意不发送 Host OK 指令给模块重置 WDT Timer，将主程序关闭或是将通讯线移除，此时会发现模块上面红色的电源指示灯会每隔 1 秒闪烁一次，正常是红色电源指示灯恒亮 . 如果主程序还在跟模块通讯，会因为一直在通讯而高速闪烁，容易误以为是恒亮。

最简单的方式当然是使用 DCON Utility 来诊断，如果已经发生 Host Watchdog Timeout，一进入模块设定画面即可看到警告信息：



Host Watchdog Timeout 以后？

在发生 Host Watchdog Timeout 后，对 DO 或是 AO 这类有输出的模块会进入安全值，这个安全值是一种锁死保护的状态。模块一旦进入安全值，在还没有解除 Host Watchdog Timeout 之前，无法改变任何输出状态，但还是能正常通讯，例如可以读取模块名称或是 DO，AO 等资料，任何尝试改变 AO 或是 DO 输出值都无法改变输出的状态。

一般会遇到上面的问题，主要是因为不了解 Host Watchdog 及安全值的搭配使用方法，或是不小心去启动主机看门狗计时器，导致现场人员无法理解为何系统无法正确输出。

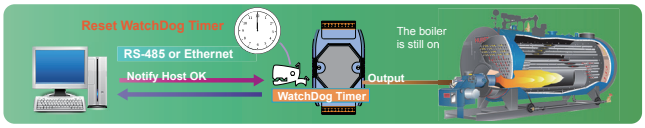
安全值设定

那什么是安全值？

所谓安全值就是输出模块在一段时间无法接受到控制台的命令时 (Host Watchdog timeout)，模块自动切到安全的输出状态 (安全值)，以确保在安全的输出状态时，预设的安全值就是没有任何输出。

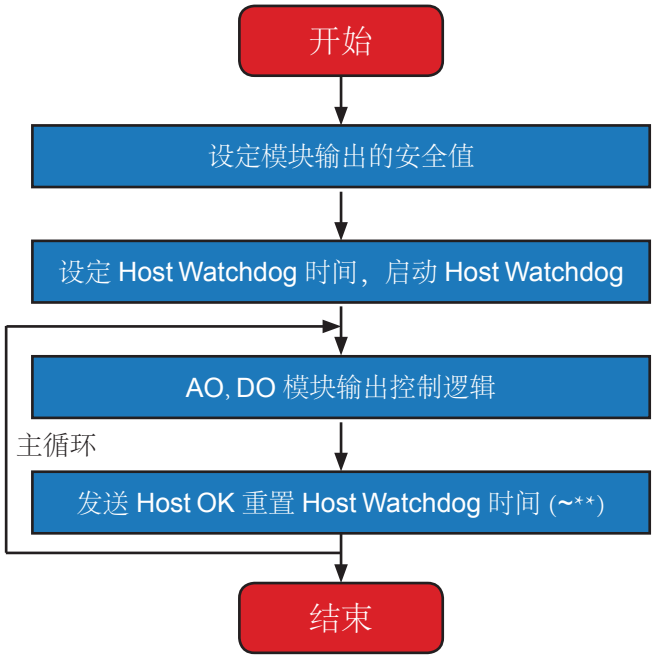
实际上安全值是按照现场的需求来设定的，例如关闭加热器，同时将现场警示灯信号或警报号响启动，现场人员才得以对系统进行通讯检测维修，将通讯问题排除。

假设系统的安全值设定为关闭输出，通讯正常状况下，程序可以随时下达命令去控制远程设备，例如将锅炉热源开启或关闭。



若当锅炉加热过程中因为通讯突然出问题，模块将无法接收到任何来自控制端的命令，此时模块的主机看门狗会发生超时，模块会自动进入安全值状态，将锅炉热源关闭，这样就能有效避免通讯发生问题时，远程模块无法接受正确控制而发生意外。

我们将上面的说明整理后，加上安全值及主机看门狗机制，原本的程序设计架构调整后如下图所示：



解除主机看门狗超时状态

实际上如果设置了主机看门狗及安全值的状况，系统只会在遇到通讯出问题时，才会发生主机看门狗超时及进入安全值状态，在通讯恢复后程序必须先解除锁定状态，系统才能恢复正常输出控制。但每当主机看门狗发生超时后，必须对模块再一次重新设置启动主机看门狗计时器，这样，模块的主机看门狗计时器才能重新运作。

因此程序需要增加对模块主机看门狗状态进行监控，如果读回的状态显示主机看门狗状态正常，则允许进入输出的控制逻辑，如果判断已经延时，则必须清除看门狗超时标志，并重新设置启动主机看门狗计时器。以下是最终修正后的程序架构：