

FDA 21 CFR Part 11 合規指南

UM019002T_20240319



介紹.....	3
FDA 21 CFR PART 11 規範.....	4
指南.....	9
進階安全模式	9
物件安全類別	9
使用者權限設定	10
使用者登入/登出	11
線上變更	12
安全設定防護	12
事件登錄狀態位址	13
其他注意事項	14
巨集指令與物件的安全防護.....	14
操作記錄	16
設定	16
備份檔案完整性	17
電子簽名	17
安全與操作記錄	17
手寫簽名	19
資料取樣與事件登錄	20
記錄保留	20
歷史檔案	20
備份檔案完整性	21
資料庫伺服器	21
一般資料完整性.....	21
系統開發與管理.....	23
系統暫存器	24

設定初始狀態	25
實務操作	27
參考資料	27

介紹

人機介面 (HMI) 與電腦控制系統在現今的製造體系中已是不可或缺，這類系統產生的電子記錄也越形重要。然而，電子記錄較容易竄改，因此需要制定規則，以保持其完整性。

FDA 21 CFR Part 11，是美國食品與藥物管理局 (FDA) 所制定，定義了電子記錄與電子簽名的標準處理程序，使其有效性與紙本記錄相同。**FDA** 監管權限的範圍非常廣泛，其中 **Part 11** 對生命科學行業的所有電腦系統都有影響。

本文件旨在幫助使用者了解如何在遵守 **FDA 21 CFR Part 11** 的前提下使用 **Weintek HMI**。在文件中，將會以 **HMI** 為主，逐一檢視 **Part 11** 法規，並討論有助於滿足要求的相關功能和設置選項。如果在受監管的环境中使用帶有 **Weintek HMI** 的系統，則會要求使用者根據本文中的指南建立和管理系統。

在此建議使用者，**FDA 21 CFR Part 11** 規範了整個工程項目，而非僅限於 **HMI**。**HMI** 的功能可以容易地使 **HMI** 所產生的電子數據符合規範，但若僅使用本文中所提及的設定，無法保證工程項目中的所有環節皆符合 **FDA 21 CFR Part 11** 的規定，必須由該領域的專業人員對整個系統進行全面審核。然而，如果以使用 **HMI** 產生任何電子資料，則應遵循本文件中的步驟。

FDA 21 CFR Part 11 規範

本章節詳細檢視了 FDA 21 CFR Part 11 的各項規定，並加入備註說明關於 HMI 的合規性。

Subpart B—電子記錄

Sec. 11.10 封閉系統的控制	是否適用?	備註
使用封閉系統來建立、修改、維護、傳輸電子記錄的人員，有設計程序與控制項以確保電子記錄從建立到接收時的真實性、完整性與適當的機密性，並確保簽署者無法輕易否認簽署的真實性。此類程序和控制項應包含以下內容：		
(a) 驗證系統以確保準確性、可靠性、持續穩定性能，並且具有識別非法記錄或被竄改記錄的能力。	否	系統驗證應由使用者完成，因為個案間的標準不盡相同。
(b) 能夠產生精確、完整並且適合 FDA 檢查、審查與複製的可讀與電子形式的記錄副本。 若人員對於 FDA 執行相關審查與複製電子記錄副本的能力，有任何問題，應聯絡該機構。	是	記錄以專有的二進制或 <code>sqlite</code> 資料庫格式儲存，並且可以使用提供的工具轉換為可讀的形式。
(c) 在整個記錄保存期間，保護記錄以便使得它們能夠提供精確而迅速的被取得。	是	提供冗餘功能。
(d) 限制只有授權人員才能存取。	是	進階安全模式能管制使用者存取 HMI。
(e) 使用安全、電腦產生的時間戳記審計跟蹤，可獨立記錄操作員建立、修改或刪除電子記錄的動作的日期與時間。 記錄更改不可模糊以前記錄的資訊。此類審計跟蹤文件的保留期限應至少與主題電子記錄所要求的期限一致，並應可供 FDA 審查與複製。	是	所有在螢幕上的操作及其詳細資訊都可以記錄在操作記錄中，並可以在 HMI 上或通過資料庫工具進行檢查。檔案紀錄可使用校驗和，以確保資料完整性。
(f) 使用操作系統檢查以強制執行允許的步驟與事件序列。	是	操作邏輯和步驟順序是 HMI 工程檔案設計不可或缺的一部分，它結合了視窗設計，邏輯控制，進階安全模式和巨集命令。
(g) 使用機構檢查以確保只有授權個人能夠使用系統、對記錄進行電子簽名、存取操作或電腦系統輸入/輸出裝置、變	是	使用進階安全模式適當設計的工程檔案可確保系統僅由授權人員存取，且應該有其他安全性

更記錄，或者執行手邊的操作。		政策來實現對 HMI 的存取控制。
(h) 系統允許使用裝置檢查，以確定資料輸入來源或操作說明的有效性。	是	進階安全模式允許使用者身份驗證，因此可以驗證與使用者相關的資料輸入來源。此外，可透過工程檔案設計進一步檢查資料來源的有效性。
(i) 確認開發、維護或使用電子記錄/電子簽名系統的人員接受過執行其指派工作的教育、培訓與經驗。	否	使用者應確保使用該系統的人員具備適當的資格。
(j) 書面政策規定根據個人電子簽名指出其承擔責任以及負責的行動，以便判定記錄與簽名是否偽造。	否	使用者應訂立具約束力的政策，並實施以及遵守與電子簽名相關的規定。
(k) 對於系統文件有適當的控管，包括：		
(1) 適當控管系統作業與維護的文件散佈、存取與使用。	是	Weintek 官方網站提供了最新的 Weintek HMI 使用手冊。使用者應負責與自有系統相關的說明文件。
(2) 修訂與變更控管程序以維持文件時間順序發展與系統文件修改的審計追蹤。	否	使用者應負責相關的修訂與變更控管程序。

Sec. 11.30 開放系統的控制	是否適用?	備註
<p>使用開放系統來建立、修改、維護、傳輸電子記錄的人員，應設計程序與控制項以確保電子記錄從建立到接收時的真實性、完整性與適當的機密性。</p> <p>這些設計程序與控制項應包含在§11.10 所述內容，如果合適，並有額外措施例如文件加密與使用適當數位簽名標準，以確保在此類情況下所需，記錄的真實性、完整性與機密性。</p>	否	對於開放系統，使用者必須建立並遵守與管理資料安全性和完整性相關的法規，並且應該將存在的各種遠端存取系統列入考慮。

Sec. 11.50 電子簽名呈現	是否適用?	備註
(a) 簽名電子記錄應清楚地包含以下所有的相關簽名資訊：	是	電子簽名功能可使用操作記錄與進階安全模式達成。
(1) 簽名者的姓名。		

(2) 簽名日期與時間。		
(3) 與簽名有關的意義 (例如審查、核准、職責或著作者身分)。		
(b) 在本節段落(a)(1), (a)(2)和(a)(3)中所發現的項目應受到與電子記錄相同控制項的約束，並且被包括為任何可讀取形式的電子記錄的部分。(例如電子顯示或列印件)	是	電子簽名功能可使用操作記錄與進階安全模式達成。

Sec. 11.70 簽名/記錄連結	是否適用?	備註
電子簽名與手寫簽名與其各自電子紀錄連結，以確保無法消除、複製或轉移簽名，以透過普遍方式偽造電子記錄。	是	安全驗證可結合簽名程序，以達成此項規定。在操作記錄資料庫中所記錄的資料應被保護而不被任意修改。

Subpart C—電子簽名

Sec. 11.100 一般要求	是否適用?	備註
(a) 每個電子簽名應對應於單一個人，不會重複給其他人使用或是重新指定給其他人。	否	使用者應確認現有的安全項目設定不被更改。
(b) 組織在建立、指定、驗證、證明或批准個人的電子簽名，或是該電子簽名的任何元件之前應驗證該個人的身分。	否	使用者所屬機構應在製成電子簽名前先執行身分確認，且只能在確認身分後，使用者才被提供登入憑證。
(c) 使用電子簽名的人員，在使用前或使用時應向本局提供證明，在其系統中的電子簽名 (在 1997 年 8 月 20 日當天或之後使用) 與傳統手寫簽名具有同等法律約束力。	否	使用者在使用電子簽名前應先報備主管單位。
(1) 這類證明需以紙本形式提出，並應該附上手寫簽名，交與辦理地方業務的辦公室(HFC-100), 5600 Fishers Lane, Rockville, MD 20857	否	使用者應提交簽名的認證給主管單位。
(2) 使用電子簽名的人員在本局提出要求時，會提供其他證書或證據，證明特定的電子簽名與簽名	否	使用者在主管單位要求時應提供資料。

者的手寫簽名具有同等法律約束力。		
------------------	--	--

Sec. 11.200 電子簽名和控制項	是否適用?	備註
(a) 非建立在生物識別技術的電子簽名應當：		
(1) 採用至少兩項獨特的識別方式，例如身分代碼與密碼。	是	進階安全模式要求使用者 ID 與密碼以利進行身分驗證。
(i) 當個人在受管制系統存取的單一、連續期間執行一系列簽署時，使用所有電子簽名元件執行第一個簽名。後續簽署應使用至少一個為僅限本人使用的電子簽名元件。	是	任何登入嘗試都應要求使用者名稱與密碼，可以透過設計工程檔案強制執行。 其他登入方式 (使用索引暫存器) 允許僅用密碼登入。
(ii) 當個人在受管制系統存取的單一、連續期間並未執行一個或多個簽署時，應使用所有電子簽名元件執行每個簽署。	是	任何登入嘗試都應要求使用者名稱與密碼。
(2) 僅會由真正的所有者所使用。	否	使用者有責任滿足這項要求。
(3) 確保非真正所有者嘗試使用個人的電子簽名時，需要有兩個或更多個人的共同合作才能達成。	否	系統管理者應建立相關協議來應對這類情形。
(b) 根據生物識別技術設計電子簽名，以確保真正所有者以外的任何其他人士皆無法使用。	否	如果使用指紋等生物識別機制登入，則使用者應負責相關安全措施。

Sec. 11.300 身分代碼控制	是否適用?	備註
使用電子簽名的人員在使用合併身分代碼與密碼的組合時，應採取適當的控制項以確保安全性與完整性，控制項包括以下：		
(a) 有適當的控制項以維持每個身分代碼與密碼組合的唯一性，使得不會有任何兩個個人擁有相同的身分代碼與密碼的組合。	是	進階安全模式設定能夠偵測使用者 ID 與密碼，且不允許重複的記錄。
(b) 有適當的控制項以確保定期檢查、撤銷或修改身分代碼與密碼發佈 (例如密碼	是	在預設情況之下，臨時帳戶有有效期限。其他密碼管理方式

過期)。		可由使用者自行定義。
(c) 有程序可透過電子形式取消授權遺失、失竊、缺少或可能危及支持或產生身分代碼或密碼資訊的權杖、卡片以及其他裝置，並且使用合適的嚴格控制核發臨時或永久替代項目。	否	使用者應建立與執行資料遺失時的相關程序。
(d) 有適當的交易防護，以避免未經授權使用密碼和/或身分代碼，並且即時與緊急偵測並向適當使用者高層報告發現未經授權使用系統安全裝置的企圖。	是	失敗的登入嘗試可被記錄為事件，而能夠用各種方式發出通知。
(e) 有用於最初和定期測試的控制項，例如可支持或產生身分代碼或密碼資訊的權杖、卡片，以確保它們運作正常，並且不會遭到未經授權的篡改。	否	使用者應定期測試以確保設備的功能性和完整性。

指南

以下介紹在 **FDA 21 CFR Part 11** 規範下使用 **Weintek HMI** 時須注意的相關功能，例如：進階安全模式、操作記錄、資料取樣、事件登錄等，以及一般設計工程檔案時的技巧和系統管理原則。

進階安全模式

進階安全模式能對使用者身分進行驗證，以達控管 **HMI** 使用權限的目的。

設定與原則：

- 賦予可操作物件不同的安全類別
- 賦予每個使用者可以操作的安全類別

依上述設定原則，進階安全模式提供個別物件權限控制，大幅增加工程檔案設計的彈性。
(Sec 11.10)

物件安全類別

各種物件的安全類別可在其屬性設定視窗的 **[安全] 頁籤 » [使用者限制]** 中分別設定。一個物件只能屬於一種安全類別，可選擇的類別為 **A, B, C...L** 等，以及一個管理員。



物件類別設定

使用者權限設定

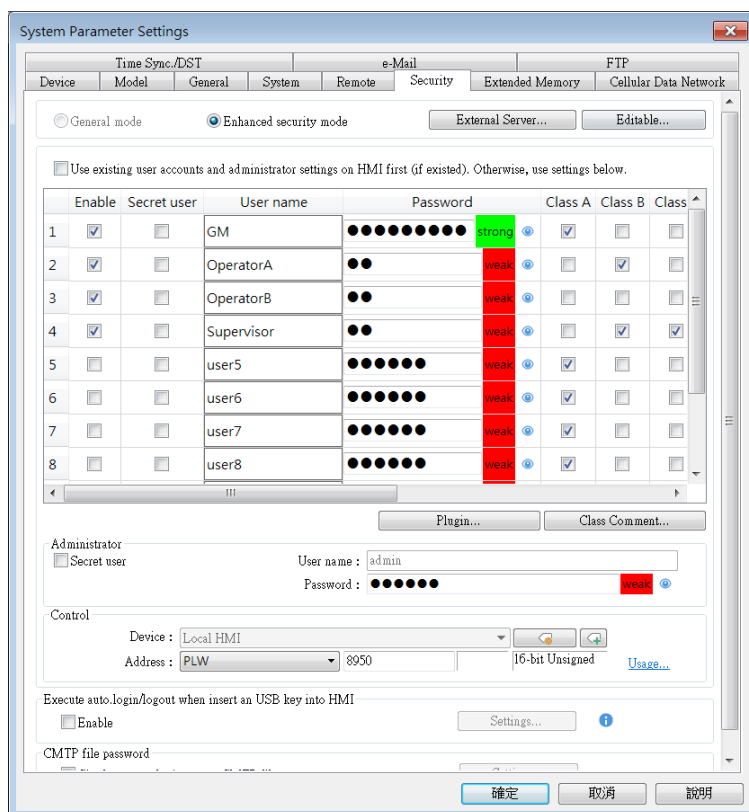
在 [系統參數設定] 的 [使用者密碼] 頁籤中，能進行安全防護設定。請使用進階安全模式，因為一般模式中缺少符合 21 CFR Part 11 的相關功能。

在此設定頁中，使用者帳戶資訊，包含是否啟用、是否為隱藏使用者、使用者名稱、密碼、被授權操作的類別等，皆可設定。**在此設定頁，使用者名稱的唯一性皆會被檢查 (Sec 11.300)，且密碼的複雜性會被評估。**

針對 cMT/cMT X 系列 HMI，為了實現使用者帳戶的集中管理，使用者認證也可以在外部伺服器上進行。該伺服器可以是另一台 HMI 或是 Active Directory(透過 LDAP)。當使用此功能時，使用者帳戶授權資訊將從外部伺服器獲取，因此外部伺服器上的授權設定應正確反映每個使用者適當的授權類別。另外，使用者認證也可以透過指紋辨別或刷智慧卡等方式進行，作為使用名稱與密碼登入之外的選擇。

管理員擁有操作所有物件類別的權限，且永遠啟用，因此，為了安全考量，應該將管理員密碼預設密碼變更。另外，將管理員設定為隱藏使用者，以防止其出現在任何項目選單中。

控制位址在安全模式中扮演了重要角色，在此設定頁中，也能設定控制位址的起始位址。



[系統參數設定] 中的進階安全模式

使用者登入/登出

所有線上操作，包含登入、登出、帳號管理，皆須使用控制位址。控制位址為使用者指定的 LW 字元位址。以下表格列出各控制位址的功能，以 LW-n 為起始位址，其中 n 為 EasyBuilder Pro 中指定的起始位址。

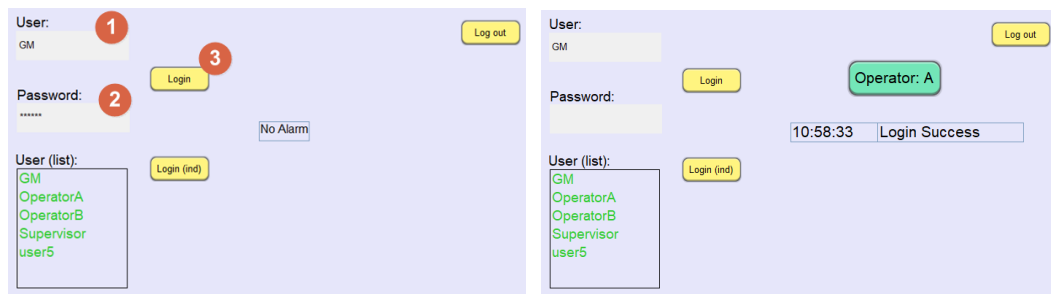
控制位址	長度	實際 LW 位址 ， n=8950	標籤名稱	描述
LW-n	1	8950	命令	控制各項操作命令 (例如: 登入，登出，新增/修改/刪除帳號...等等)。
LW-n + 1	1	8951	命令執行結果	顯示執行命令的結果。
LW-n + 2	1	8952	使用者索引	帳號索引 (配合項目選單物件使用)。
LW-n + 3	1	8953	使用者權限	權限值 (Level A = bit0, Level B = bit1...等等)。
LW-n + 4	8	8954~8961	使用者名稱	帳號名稱 (可為英文字母或數字，大小寫視為不同)。
LW-n + 12	8	8962~8969	密碼	帳號密碼 (可為英文字母、數字、符號，大小寫視為不同)。

範例 1: 登入

欲登入，需先分別在對應的暫存器中，輸入使用者名稱與密碼，然後在【命令】位址中下達操作指令。

步驟	動作 (LW-n=8950)
1. 在【使用者名稱】位址輸入名稱。	在起始位址 LW-8954~輸入使用者名稱
2. 在【密碼】位址輸入密碼。	在起始位址 LW-8962~輸入使用者密碼
3. 在【命令】位址中輸入數值 1，下達登入命令。	在 LW-8950 輸入數值 1

系統會依照各暫存器中的資料驗證使用者名稱與密碼。確認後，使用者即登入，且能檢視或是操作被授權的物件。



登入前 vs. 登入後

範例 2: 登出

1. 如欲登出，只需在 [命令] 位址輸入數值 3，即可下達登出指令。

使用者名稱與密碼組合在登入時是必要的。(Sec 11.200)

另外，所有的使用者也能列入下拉選單，於登入時選擇後僅需輸入密碼。

建議只有在“單次的輔助性身分認證”時，才使用索引方式，以符合 Sec 11.200

欲了解控制位址的詳細介紹及其功能，請見 EasyBuilder Pro 使用手冊第十章。

線上變更

除了在使用 EBPro 設計工程檔案時設定使用者帳號、密碼、權限等，帳號管理也可線上在 HMI 進行。線上允許的操作包括：更改密碼、新增/更改臨時帳戶，新增/更改到期帳戶，新增/刪除與帳戶關連的指紋/智慧卡，以及更改使用者權限等。**使用者可以使用到期帳戶來定期回復或更新帳號，以解決帳戶過期的問題。(Sec 11.300)**

透過設定控制位址以及使用適合的控制物件即可達到線上使用者帳戶管理，詳細介紹請參閱 EasyBuilder Pro 使用手冊第十章。

安全設定防護

啟用“唯讀”模式能在他人取得原始工程檔案時，仍防止未經授權的使用者進行安全設定。在唯讀模式中，安全設定不能被變更，且密碼會使用星號(*)顯示，以防止密碼外流。必須使用原始設定的密碼也才能重新取得管理權限。

系統參數設定

802.1X (WiFi) WiFi 熱點 時間同步/夏令時間 郵件 FTP

設備 HMI 屬性 一般屬性 系統 遠端 使用者密碼 擴展記憶體 行動網路

☐ 一般模式 ☒ 進階安全模式 外部伺服器... 唯讀...

☐ 在 HMI 上使用現有的使用者帳號和管理員設定 (若已存在), 否則將使用以下設定

啟用	隱藏使用者	使用者名稱	密碼	類別 A	類別 B	類別 C	類別 D
<input checked="" type="checkbox"/>	<input type="checkbox"/>	General	●●●●●●●●	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	OperatorA	●●●●●●●●	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	OperatorB	●●●●●●●●	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	SiteSupervisor	●●●●●●●●	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	user5	●	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	user6	●	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	user7	●	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	user8	●	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

管理員
☒ 隱藏使用者 使用者名稱: admin 密碼: ●●●●●●

唯讀模式

事件登錄狀態位址

狀態位址 (LW-n+1) 能顯示任何使用者操作後，命令執行的結果。狀態位址所顯示的數值，能用來確認登入狀況，或回報登入時產生錯誤的原因。

當偵測到異常的登入操作時，能根據回報做出反應。(Sec 11.300)

要實現以上目的，使用者需先建立新的事件登錄物件，並指定讀取位址為 LW-n+1，[命令執行結果]。在 [訊息] 頁籤下的 [內容] 部分，使用者能夠輸入訊息內容，該內容將顯示於事件登錄物件中，使閱者更容易了解回報的狀態。

事件登錄

一般屬性 訊息 統計

類別: 1: Category 1

等級: 高

HMI 重置時監視事件的延遲時間: 1 秒

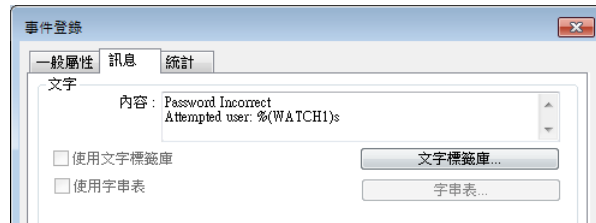
☒ 推播通知 (EasyAccess 2.0)

類型: ☐ 位元 ☒ 字組

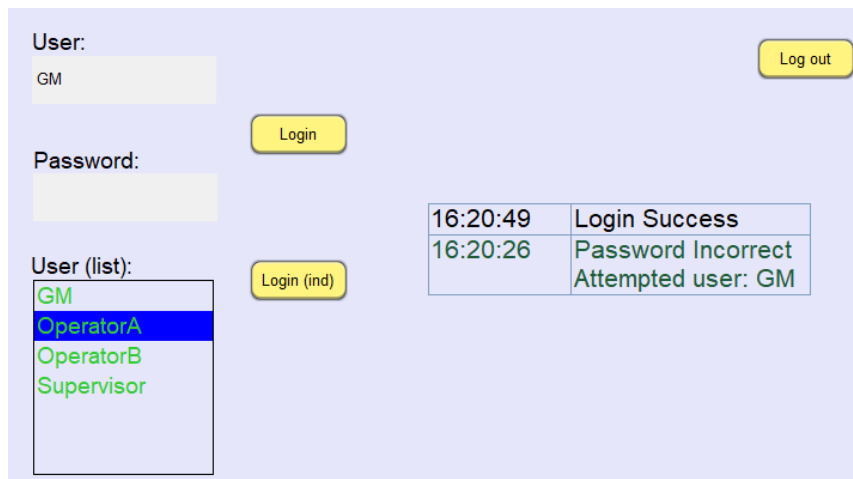
讀取位址: 設備: Local HMI 位址: LW 8951 16-bit Unsigned

通知: ☒ 啟用

觸發條件: 狀態: 16 ☐ 動態狀態數值



事件登錄顯示命令執行結果



事件登錄顯示登入結果

其他注意事項

請定期或是在每次登入後，清空用戶名稱與密碼，以預防他人使用。同樣的，使用自動登出（可在系統參數設定啟用）來預防忘記登出時，發生未經授權的操作。

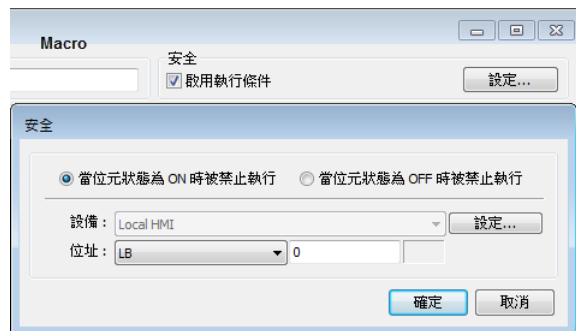
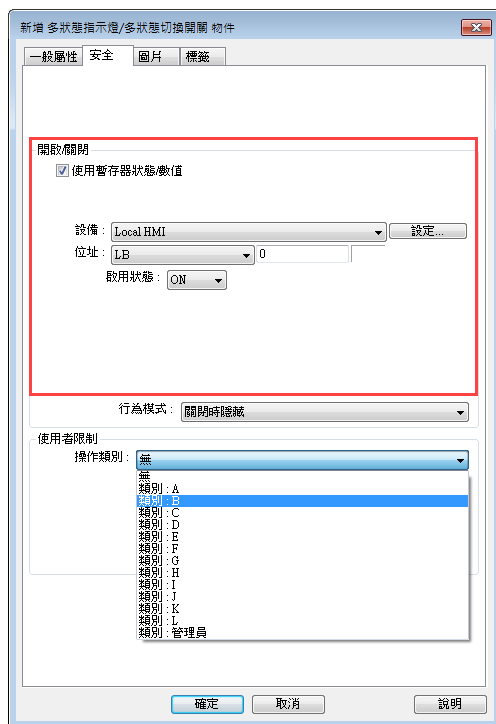
使用威綸 HMI 的安全防護功能，即符合 FDA 21 CFR Part 11 之規定，但仍可能在某些情況下，無法完全滿足規範要求。使用者必須建立適當的標準操作程序並訂立嚴格的使用方針。

使用方針可包括以下要點，但並非限定在以下內容。

- 經過授權的帳戶擁有者必須使用自己的帳戶密碼來登入系統。
- 使用者有責任保護其登入憑證。使用者間分享登入憑證應被嚴格禁止，這包含但不限於帳戶名稱/密碼以及智慧卡等。
- 需設定強度足夠的密碼，包含至少一個數字和一個特殊字元。請避免使用慣用詞作為密碼或密碼的一部分。

巨集指令與物件的安全防護

除了物件類別設定，物件與巨集指令皆可個別設定安全防護，使其能夠在指定的位元暫存器狀態變為 ON/OFF 時，被啟用或關閉。若使用這類防護，物件能夠在不被允許操作時，被關閉或不顯示。而巨集指令如啟用安全防護時，即使觸發條件已經達成，巨集仍不會被觸發執行。



物件與巨集指令的安全設定頁面。

操作記錄

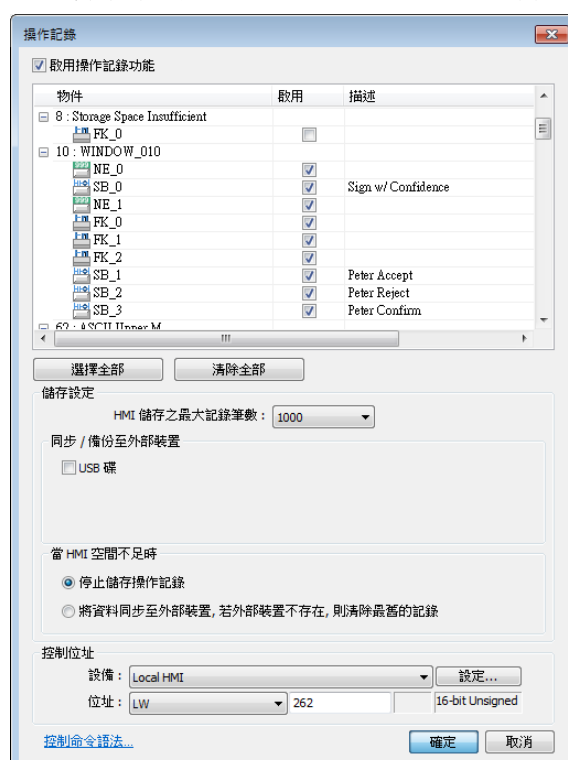
當對物件執行任何操作，操作記錄能記錄所有關於該動作的資訊，包括：日期/時間、使用者名稱、物件類別、視窗編號、物件名稱、使用者定義的描述、動作(物件種類)、位址、以及變更資訊。操作記錄若正確設定，應能滿足對於審計追蹤與電子簽名的要求。(Sec 11.10)

開始記錄後，操作記錄會預設以 **sqlite** 資料庫格式儲存在 HMI 記憶體中，也能備份至連接的外部裝置中，例如 **USB 硬碟**。另外，備份的操作記錄檔案也可以包含校驗和 (checksum)，以確保資料的完整性。

威綸提供的 **EasyConverter** 工具能在電腦上開啟 **sqlite** 檔案，以顯示操作記錄資料，並支援將檔案輸出為 **PDF/Excel/CSV** 格式。而在各種輸出格式之中，應盡可能選擇以 **PDF** 格式輸出。若備份檔案含有校驗和(checksum)，**EasyConverter** 可以驗證校驗和，確認資料的完整性。

設定

在 [物件] » [操作記錄] » [操作記錄設定] 能啟用操作記錄功能。選擇所有需記錄操作過程的物件，並寫下關於該物件執行動作的描述。這些描述也會一併記錄在操作記錄中。



操作記錄設定

提示：點選漏斗圖示能指定欲檢視的物件

使用者需注意此頁的設定，若未詳細設定，資料可能遺失。在將外部記憶體的資料同步之前，請確認 HMI 記憶體之最大記錄筆數，以免超過。請同時將資料同步至 USB 硬碟中，以便在 HMI 空間不足時，作為備用，以防資料流失。

如同前章說明的安全模式，操作記錄也使用控制位址，以便在 HMI 運行時，對操作記錄下指令，或是確認與操作記錄相關的狀態報告。請謹慎使用控制位址，避免意外清除資料，或是關閉操作記錄，並且盡可能通報所有執行結果。

如欲檢視操作記錄，可在螢幕上放置一個操作記錄檢視物件。

備份檔案完整性

欲確保備份資料完整性，使用者可以在操作記錄備份檔案中添增校驗和(checksum)。在產生備份檔案時勾選 [啟用校驗和以確保資料完整性]，即可啟用此功能。此功能只支援於 cMT/cMT X 型號。



備份物件校驗和設定

EasyConverter 可用於檢驗操作記錄備份檔案內容的完整性。若檢驗時發現檔案可能已被竄改，EasyConverter 將發出警示。

電子簽名

以下範例介紹如何產生電子簽名。(Sec 11.10, Sec 11.50)

安全與操作記錄

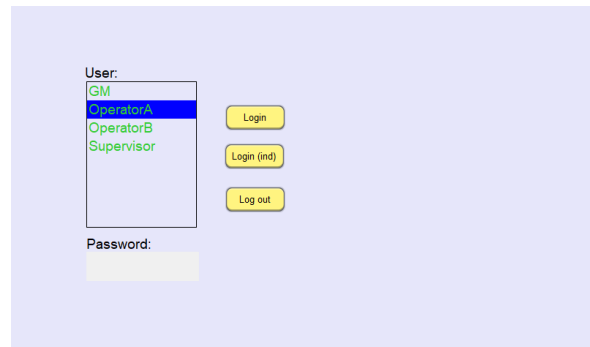
結合安全設定與操作記錄，可以記錄使用者的動作，這些記錄相當於電子簽名的效果。

範例：

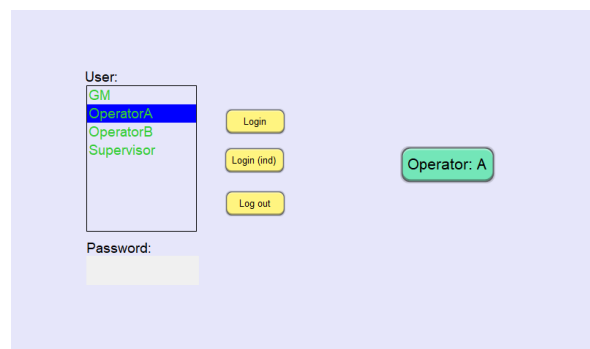
首先，建立登入頁面 (15 號視窗)，其中放置一個功能鍵，用於切換視窗至 16 號視窗。此功能鍵平時應隱藏，只在正確登入後顯示，以便確認所有在 16 號視窗進行的動作皆是經過授權的使用者所執行。接著，在 16 號視窗放置一些與簽名功能相關的動作按鈕，並記錄這些物件的操作記錄。當一個動作按鈕被觸發，其觸發時間、操作者、動作描述都會記載在操作記錄中。假設所有數據皆完整，操作記錄中的數位簽名便可視為有效。

截圖說明:

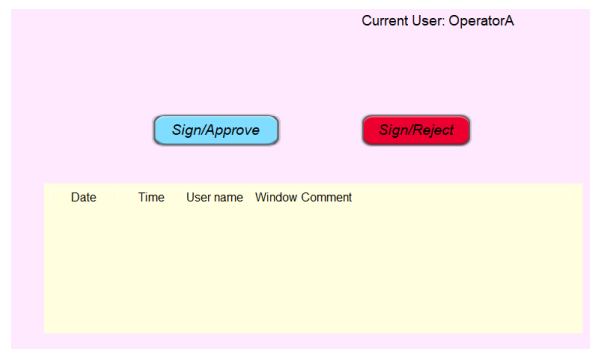
1. 在 15 號視窗，以使用者名稱以及密碼登入。



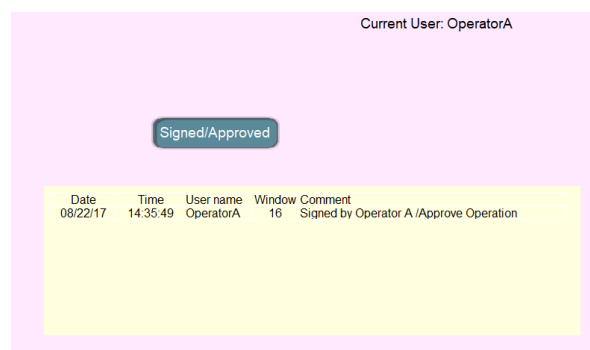
2. 登入後，能切換視窗的功能鍵即會顯示。



3. 16 號視窗有兩個按鈕，各能執行不同的動作，當按下其中一個按鈕後，另一個案鈕便會消失 (使用安全防護功能)。



4. 按下其中一個按鈕的操作記錄會顯示於操作記錄資料庫中。

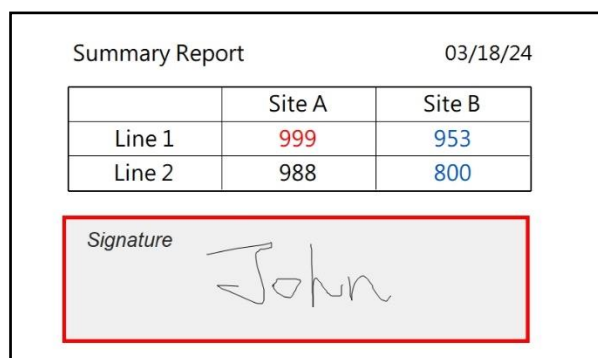


手寫簽名

JS 物件提供了一種自定功能的方式，以打造出無法使用內建元素實現的功能。使用 JS 物件，可以製作出一個數位繪圖板，讓使用者像在紙上簽名一樣簽署自己的名字。

範例：

將報告內容和以 JS 物件製作的簽名欄位放在同一頁面上，並在有人簽署後截圖螢幕。保存的螢幕截圖可被視為帶有電子簽名的報告。

The image shows a screenshot of a report page. At the top, it says "Summary Report" on the left and "03/18/24" on the right. Below this is a table with three columns: an empty header column, "Site A", and "Site B". The table has two data rows: "Line 1" with values "999" (in red) and "953" (in blue), and "Line 2" with values "988" and "800". Below the table is a signature field. It has a light gray background and a red border. The word "Signature" is written in a small font on the left. The name "John" is written in a large, handwritten-style font in the center of the field.

	Site A	Site B
Line 1	999	953
Line 2	988	800

Signature John

簽名欄位
(使用 JS 物件的 canvas 功能建立)

注意：僅 cMT X 型號支援 JS 物件。如有需求，我們可以提供包含以 JS 物件製作的簽名欄位的範例工程檔案。

本章節中的範例展示了產生電子簽名的一些實用作法，但這當然不是全部的方法。若使用類似的概念，應用巨集指令，彈出視窗等其他元素，也能得到操作體驗不同，但相同效力的電子簽名。

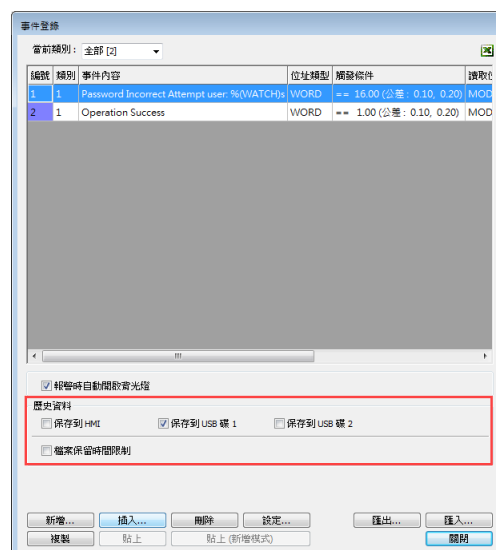
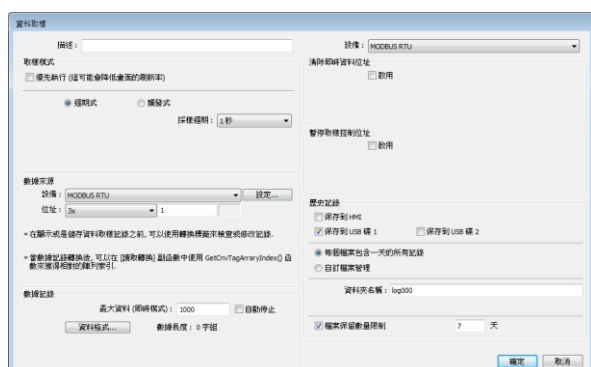
資料取樣與事件登錄

記錄保留

資料取樣與事件登錄能產生電子記錄，並將資料儲存為 dtl、evt、db 格式。與操作記錄相似的是，使用者需謹慎設定，若未詳細設定，資料可能遺失。

請務必勾選將歷史資料儲存至 HMI 記憶體或外部裝置(USB 硬碟/SD 卡)中，這可以保障在 HMI 斷電時，仍能取回資料。當工程檔案的設計中，需要高頻率地記錄大量的資料時，建議儲存在外部裝置中。請注意，供使用者選擇是否允許 FTP 客戶端存取 USB 硬碟/SD 卡中的資料的選項應該關閉，以預防資料處理錯誤。

檔案保留時間限制必須長於規範 (Sec 11.10) 制定的時間。也請定期備份至 USB 硬碟或是備份伺服器。當備份至外接伺服器時，也需遵守相關資料處理程序。

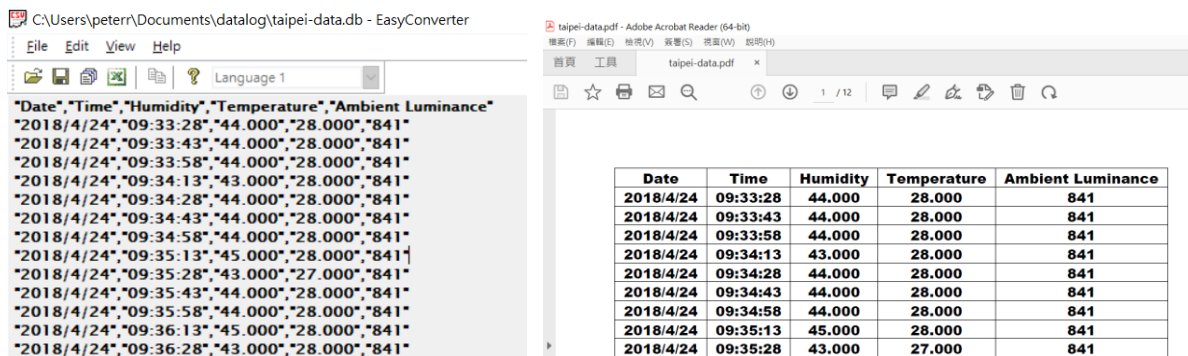


開啟歷史資料保存

歷史檔案

dtl 與 evt 的二進制和專有特性表示數據文件不易被讀取或偽造。(Sec 11.10)

威綸提供 EasyConverter 工具，以在電腦上讀取 dtl, evt, db 檔案。為了安全，請使用威綸官方發佈的工具。EasyConverter 會顯示記錄資料，並輸出檔案為 PDF/Excel/CSV 格式。使用者在處理資料時須遵守相關規定。而在各種輸出格式之中，應盡可能選擇以 PDF 格式輸出。



使用 EasyConverter 讀取 db 檔案並儲存為 PDF 檔案

備份檔案完整性

欲確保備份資料完整性，使用者可以在事件登錄或資料取樣備份檔案中添增校驗和 (checksum)。在產生備份檔案時勾選 [啟用校驗和以確保資料完整性]，即可啟用此功能。此功能只支援於 cMT/cMT X 型號。



備份物件校驗和設定

EasyConverter 可用於檢驗事件登錄或資料取樣備份檔案內容的完整性。若檢驗時發現檔案可能已被竄改，EasyConverter 將發出警示。

資料庫伺服器

當使用 cMT/cMT X 系列型號時，資料取樣、事件登錄、操作記錄資料能被同步至外部的 MySQL 或 MS SQL 資料庫。另外，cMT/cMT X 系列支援 SQL 查詢，能直接存取資料庫伺服器中的資料。即使用戶仍需注意安全問題，但若能建立一個安全且受到保護的資料庫伺服器，儲存至資料庫伺服器能作為在 HMI 上儲存檔案的替代方案。

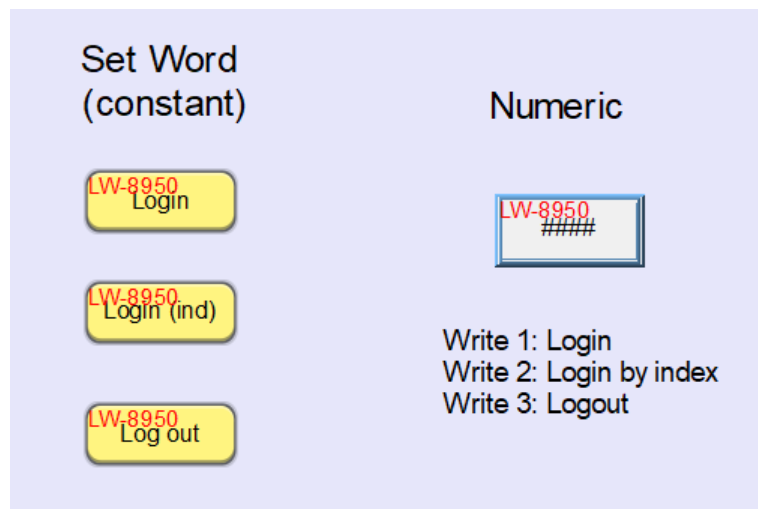
一般資料完整性

為了保持資料完整性，請限制對系統暫存器和功能控制位址的存取。意外修改這些位址可能導致不良結果。(Sec 11.70)

這些規範包含能在 HMI 上更改歷史資料的系統暫存器，進階安全模式的控制位址，操作記錄的控制位址，資料取樣，事件登錄，以及其他可能相關的功能。這表示工程檔案

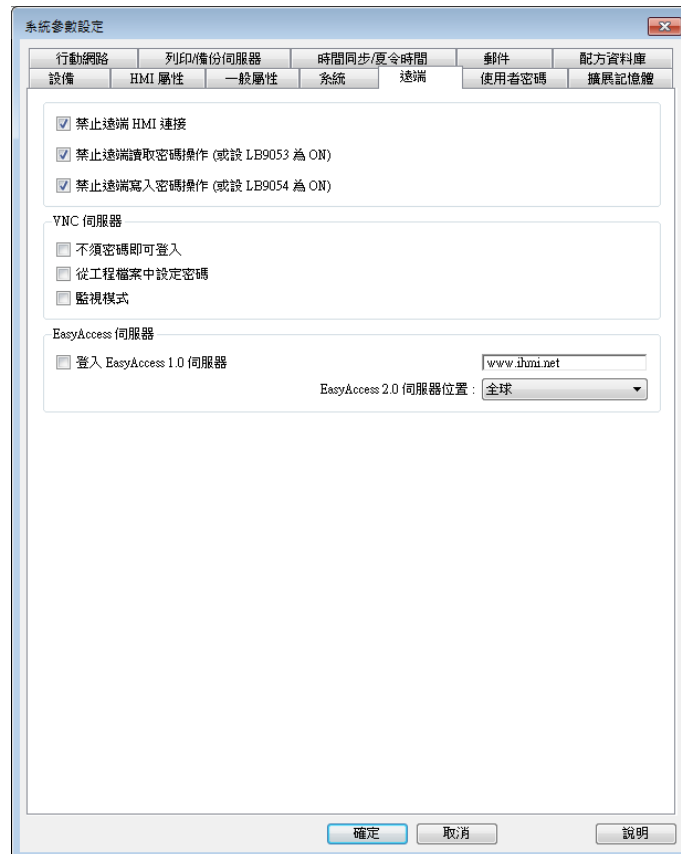
中不可放置能夠直接控制這些暫存器的物件，而且，常常被忽視的是，由外部連結也應該要被限制並且密切監視。

相較於自由調整的方式，在本地使用安全防護功能與並使用行為可預期的物件。舉例來說，使用多狀態設定物件寫入常數，而非使用數值物件。另外，請檢查可能大範圍影響暫存器的背景物件，例如巨集指令或是資料傳輸物件，以及避免未設界限地使用索引暫存器。



多狀態設定 VS 數值物件

從外部連接時，若使用到的控制位址之中，有 LW 位址，請將由遠端連接 HMI 的設定關閉（在系統參數設定，或是使用系統暫存器）。也應避免使用 MODBUS 伺服器，由於 MODBUS 伺服器的暫存器皆直接對應到 LW/LB/RW 等位址，因此任何寫入 MODBUS 伺服器的操作都可能影響這些暫存器。若控制位址是 PLC 位址，則所有 PLC 相關位址的存取條件都應該詳細檢視。



禁止遠端連線至 HMI 設定

系統開發與管理

1. 設計工程檔案時，需加入登入頁面，以便在重新啟動時，要求使用者登入方進行後續設定。登出後一定時間內，若觸控螢幕未被觸碰，應自動回到登入頁面。(Sec 11.10)
2. HMI 程式不受限制，但應有安全機制，讓使用者能依照合於規定的步驟程序操作。(Sec 11.10)
3. 只允許經過授權或合乎資格的人員進入系統，是相當重要的。若由未經訓練的人員登入系統進行操作，圖片檢視物件或是 PDF 閱讀器或許可以顯示重要的操作步驟，讓這類人員能夠立即查看。
4. 以下功能不可開啟，或是至少使用密碼防護：
 - a、遠端 HMI
 - b、PLC 控制 (換頁)
 - c、Modbus 伺服器
 - d、VNC 伺服器

- e、 cMT Diagnoser (cMT/cMT X 系列)
- f、 OPC UA 伺服器 (部分 cMT/cMT X 系列)

此列表不應視為詳盡無遺。

5. 以下密碼不應使用預設密碼，以避免未經授權的登入動作。

- a、 HMI 密碼 (下載、上傳、重置資料)
- b、 CXOB 密碼 (編譯/反編譯)
- c、 VNC 伺服器 (或啟用唯獨模式)
- d、 FTP (上傳歷史密碼)
- e、 系統設定、上傳工程檔案、歷史資料、使用者密碼 (cMT/cMT X 系列)
- f、 網頁伺服器 (cMT/cMT X 系列)、WebView (cMT X 系列)

此列表不應視為詳盡無遺。

6. 請使用密碼保護 EasyBuilder Pro 工程檔案。

7. 除了現場檢查之外，也須注意 PLC 通訊參數，以確認 HMI 連接至正確的目標機器。
在 HMI 運行時，系統暫存器可用於檢視這些參數。(Sec 11.10) 另外，也可指定啟動報警的各種條件，以利偵測任何變化。

8. 隱藏系統設定列以避免未經授權的系統設定變更，例如更改系統時間、HMI 密碼，以及其他重要的操作。

9. 請禁止對本地系統時間的寫入操作，以確保資料時間戳記的正確性。若能使用網路連線，請使用一個可信任的 NTP 伺服器，也是能確保時間戳記正確的方法。

10. 您可以隨時在威綸官方網頁下載最新的威綸人機使用手冊。www.weintek.com (Sec 11.10)

系統暫存器

以下表格列出一些相關的系統暫存器，請注意這並非詳盡的表格，且適用性可能依實際應用而不盡相同。

位址	描述
LB-9020	顯示 (設 ON)/隱藏 (設 OFF) 系統設定列
LW-9081	螢幕保護時間 (單位：分鐘)
LB-9025	刪除 HMI 記憶體裡日期最早的資料取樣檔案 (設定為 ON)

LB-9026	刪除 HMI 記憶體裡全部資料取樣檔案 (設定為 ON)
LB-9034	儲存事件記錄與取樣數據至 HMI, USB 碟, SD 卡 (設定為 ON)
LB-11949	刪除 SD 卡裡日期最早的資料取樣檔案 (設定為 ON)
LB-11950	刪除 SD 卡裡全部資料取樣檔案 (設定為 ON)
LB-11951	更新 SD 卡裡資料取樣統計資訊 (設定為 ON)
LB-11952	刪除 USB 碟 1 裡日期最早的資料取樣檔案 (設定為 ON)
LB-11953	刪除 USB 碟 1 裡全部資料取樣檔案 (設定為 ON)
LB-9022	刪除 HMI 記憶體裡日期最早的事件記錄檔案 (設定為 ON)
LB-9023	刪除 HMI 記憶體裡全部事件記錄檔案 (設定為 ON)
LB-11940	刪除 SD 卡裡日期最早的事件記錄檔案 (設定為 ON)
LB-11941	刪除 SD 卡裡全部事件記錄檔案 (設定為 ON)
LB-11942	更新 SD 卡裡事件記錄統計資訊 (設定為 ON)
LB-11943	刪除 USB 碟 1 裡日期最早的事件記錄檔案 (設定為 ON)
LB-11944	刪除 USB 碟 1 裡全部事件記錄檔案 (設定為 ON)
LW-9200~LW9260	位址索引暫存器 0~31
LB-9044	禁止遠端控制 (當狀態為 ON)
LB-9053	禁止遠端讀取密碼操作 (當狀態為 ON)
LB-9054	禁止遠端寫入密碼操作 (當狀態為 ON)
LB-9197	只允許遠端 HMI 使用檢視功能 (當狀態為 ON)
LB-9198	禁止本機 HMI 觸發巨集 (當狀態為 ON)
LB-9199	禁止遠端 HMI 觸發巨集 (當狀態為 ON)
LB-12088	啟用 VNC 監視模式 (當狀態為 ON)
LB-12092	開啟 (設 ON)/取消 (設 OFF) VNC 功能
LB-12361	操作記錄功能的狀態 (OFF: 關閉, ON: 開啟)

設定初始狀態

以上許多條件，需在啟動 HMI 之前完成暫存器數據設定，有許多方法可以完成這類設定。

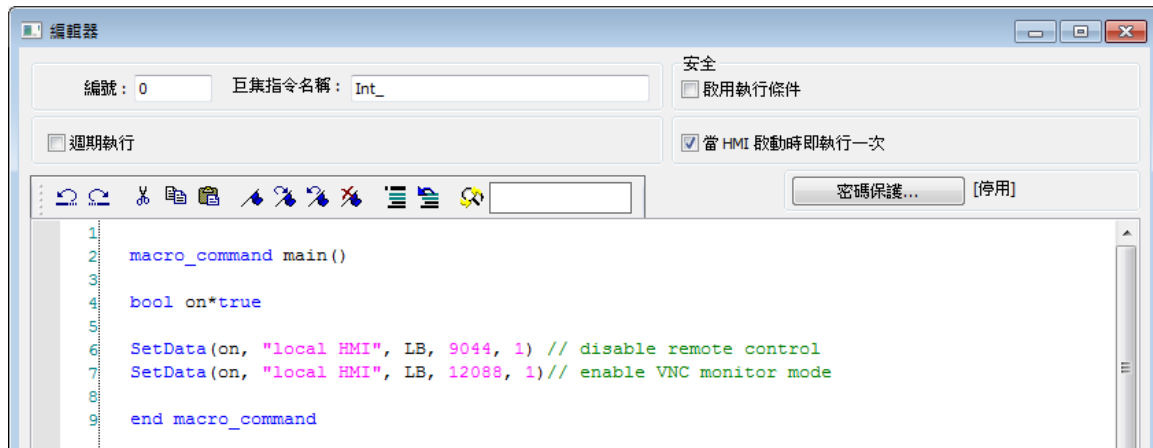
使用物件

1. 放置一個“位元狀態設定”物件，，並依據地址的特性，設定其動作為“視窗打開時設 OFF”，或是“視窗打開時設 ON”。
若使用字元暫存器，則可放置“多狀態設定”物件，並設定其動作為“視窗打開時設定”，填入適當的常數值。
2. 在開始視窗中依照系統參數設定放置各種物件，或將物件放置於公共視窗（視窗編號 4）。

使用巨集指令

1. 建立巨集指令用以設定暫存器數值。
2. 勾選“當 HMI 啟動時即執行一次”。
3. 或是在系統參數設定中，開啟系統設定頁籤，並勾選“開機後使用初始化巨集指令”，並使用前一步驟建立的巨集指令。

以下截圖展示一個巨集指令範例。此巨集指令能在 HMI 開機時，關閉遠端控制並開啟 VNC 監視模式。



巨集指令範例

實務操作

若正確設定並依照此文件的說明使用威綸 HMI，應能符合許多在 **FDA 21 CFR Part 1** 制定的規範。其他不適用於 HMI 的規範，使用者須制定程序並嚴格遵守，以符合相關規範。

參考資料

Code of Federal Regulations, Title 21. Electronic Records; Electronic Signatures. (2016)