ETC 資通訊檢測實驗室

TAF Testing Laboratory 3325

標準檢驗局指定試驗室認可編號：SL4-A2-T-0020

試驗報告指定編號：SL4A2T0020220024

報告編號：22-04-CAV-008-01

商品名稱：變流器(內嵌監視單元)（太陽能變流器）

申請人：台達電子工業股份有限公司台南分公司

生產廠場：中達電子(江蘇)有限公司

台達電子工業股份有限公司平鎮廠

廠牌：台達電子

主型式型號：M30A_230

主型式規格：AC: 400 V/380 V/50 HZ/60 HZ/30 kW

系列型號／規格：詳見檢測報告摘要

依據標準：太陽光電變流器及監視單元資安檢測技術規範（109年12月版）

試驗結果：合格

試驗場地地址：桃園市龜山區文明路29巷8號

遊測場地地址：台南市善化區環東路二段39號

報告簽署人：葉錫勳

報告發行日期：111.10.5

目 次

檢測報告摘要

報告編號	22-04-CAV-008-01		
檢測依據	太陽光電變流器及監視單元資安檢測技術規範（109 年 12 月版）		
送檢單位名稱	台達電子工業股份有限公司台南分公司		
送檢單位地址	台南市善化區環東路二段 39 號		
受測產品	主型式	變流器	廠牌：台達電子
			型號：M30A_230
			規格：AC: 400 V/380 V/50 HZ/60 HZ/30 kW
			序號：OAZ21800001W0
			韌體版本號 1：V1.20（COMM）
			韌體版本號 1 Hash(SHA1)：13e4f9b6dc3f2049d4f40903fdcd5b2b0d418c63
			韌體版本號 2：V1.16（DSP1）
			韌體版本號 2 Hash(SHA1)：82eecf26268578191624c26110c71a1e72b7c01e
			韌體版本號 3：V1.02（DSP2（ARC））
			韌體版本號 3 Hash(SHA1)：9d75e738214d1bb7ece926ccdd1074a721d0a52d
			韌體版本號 4：V1.03（RED）
			韌體版本號 4 Hash(SHA1)：591fbd1d7e5c0dbea5f0eb450d287e558fc53e2b
		內嵌式監視單元	廠牌：台達電子
			型號：RS9113-N00-S1C（WIFI）
			規格：DC 3.3V
			序號：OAZ21800001W0
			韌體版本號：V1.03（WIFI）
			韌體 Hash(SHA1)：bf4b396c9fce56d83f21c0321d6de54ad4b6fc74
	系列型式	變流器	廠牌：台達電子
			型號：M30A_231
			規格：AC: 400 V/380 V/50 HZ/60 HZ/30 kW
			序號：OAZ21800539W0

			韌體版本號 1：V1.20 （COMM）
			韌體版本號 1 Hash(SHA1)： 13e4f9b6dc3f2049d4f40903fdcd5b2b0d418c63
			韌體版本號 2：V1.16 （DSP1）
			韌體版本號 2 Hash(SHA1)： 82eecf26268578191624c26110c71a1e72b7c01e
			韌體版本號 3：V1.02 （DSP2（ARC））
			韌體版本號 3 Hash(SHA1)： 9d75e738214d1bb7ece926ccdd1074a721d0a52d
			韌體版本號 4：V1.03 （RED）
			韌體版本號 4 Hash(SHA1)： 591fbd1d7e5c0dbea5f0eb450d287e558fc53e2b
		內嵌式監視單元	廠牌：台達電子
			型號：RS9113-N00-S1C（WIFI）
			規格：DC 3.3V
			序號：OAZ21800539W0
			韌體版本號：V1.03 （WIFI）
			韌體 Hash(SHA1)： bf4b396c9fce56d83f21c0321d6de54ad4b6fc74
	系列型式	變流器	廠牌：台達電子
			型號：M20A_220
			規格：AC: 400 V/380 V/50 HZ/60 HZ/20 kW
			序號：OCE21700249W0
			韌體版本號 1：V1.20 （COMM）
			韌體版本號 1 Hash(SHA1)： 13e4f9b6dc3f2049d4f40903fdcd5b2b0d418c63
			韌體版本號 2：V1.16 （DSP1）
			韌體版本號 2 Hash(SHA1)： 82eecf26268578191624c26110c71a1e72b7c01e
			韌體版本號 3：V1.02 （DSP2（ARC））
			韌體版本號 3 Hash(SHA1)： 9d75e738214d1bb7ece926ccdd1074a721d0a52d
			韌體版本號 4：V1.03 （RED）

			韌體版本號 4 Hash(SHA1)： 591fbd1d7e5c0dbea5f0eb450d287e558fc53e2b
		內嵌式監視單元	廠牌：台達電子
			型號：RS9113-N00-S1C（WIFI）
			規格：DC 3.3V
			序號：OCE21700249W0
			韌體版本號：V1.03 （WIFI）
			韌體 Hash(SHA1)： bf4b396c9fce56d83f21c0321d6de54ad4b6fc74
系列差異分析	本系列機種主要差異在於 PV String 數量不同，此差異並不影響資安，詳如附件二。		
資安等級	□1 級 ■2 級		
檢測結果	■合格□不合格 □其他_____		
樣本收件日期	111 年 08 月 01 日		
驗測起始日期	111 年 08 月 01 日		
驗測完成日期	111 年 09 月 28 日		
報告日期	111 年 10 月 05 日		
實驗室測試能量	認證編號：3325		
認證有效期間	109 年 4 月 25 日 至 112 年 4 月 25 日		
認證範圍	本檢測涵蓋「太陽光電變流器及監視單元資安檢測技術規範（109 年 12 月版）」		
備註	本報告僅對受測樣品負責，未經本中心書面許可不得部份複製本報告，完整複製則不在此限。 本檢測程序依「太陽光電變流器及監視單元資安檢測技術規範」所訂定的檢測項目進行測試及判定，測試項目為非定量試驗，其量測不確定度不影響報告符合性判定之結果，故不適用。		

實驗室主管(簽章)	報告簽署人(簽章)	檢測人員(簽章)
劉文相	葉錫勳	吳建成

1. 檢測結果摘要表

表 1 檢測結果摘要

資安構面	檢測方法		檢測結果	資安等級	
	編號	內 容		1 級	2 級
1.1 實體資安	1.1.1	實體防護	■符合 □不符合		V
1.2 系統資安	1.2.1	軟/韌體更新機制	■符合 □不符合	V	V
	1.2.2	軟/韌體安全性評估	■符合 不符合		V
1.3 身分鑑別	1.3.1	人機介面身分鑑別(實體)	□符合 □不符合 ■不適用	V	V
	1.3.2	人機介面身分鑑別(無線)	□符合 □不符合 ■不適用	V	V
2.1 實體資安	2.1.1	實體防護	■符合 □不符合		V
	2.1.2	最小實體介面要求	■符合 □不符合	V	V
2.2 系統資安	2.2.1	已知脆弱性掃描	■符合 □不符合	V	V
	2.2.2	軟/韌體更新機制	■符合 □不符合	V	V
	2.2.3	軟/韌體安全性評估	■符合 □不符合	V	V
	2.2.4	機敏資料保護	□符合 □不符合 ■不適用	V	V

資安構面	檢測方法		檢測結果	資安等級	
	編號	內 容		1 級	2 級
	2.2.5	惡意程式防護	■符合 □不符合		V
	2.2.6	帳戶管理	■符合 □不符合	V	V
	2.2.7	事件日誌	■符合 □不符合	V	V
	2.2.8	事件日誌之儲存容量與效期	■符合 □不符合		V
2.3 身分鑑別	2.3.1	最小通訊埠要求	■符合 □不符合	V	V
	2.3.2	動態資料加密保護	■符合 □不符合 □不適用	V	V
	2.3.3	動態資料加密保護-進階	■符合 □不符合		V
	2.3.4	封包流量與指向分析	■符合 □不符合	V	V
2.4 身分鑑別	2.4.1	人員使用者識別與鑑別	■符合 □不符合	V	V
	2.4.2	通行碼強度(長度基礎)	□符合 □不符合 ■不適用	V	V
	2.4.3	通行碼輸入頻次限制	□符合 □不符合 ■不適用	V	V
	2.4.4	預設通行碼變更機制	□符合 □不符合 ■不適用	V	V

2. 檢測環境

2.1.檢測場地

- 測項 1.1.1～1.3.2 及 2.2.3 之遊測場地為台達電子工業股份有限公司台南分公司
  (地址：台南市善化區環東路二段 39 號)
  環境溫度/相對濕度：攝氏 27.5 度 / 63% R.H.

- 其餘測項之檢測場地為財團法人台灣商品檢測驗證中心資通訊檢測實驗室
  (地址：桃園市龜山區文明路 29 巷 8 號)
  環境溫度/相對濕度：攝氏 22.3 度 / 65% R.H.

2.2.檢測佈局

變流器及內嵌式監視單元資安檢測工具安裝於測試電腦，包括弱點掃描工具、靜態程式碼分析工具、網路偵測工具與網路封包偵錄工具等。

本檢測佈局為：待測物連接至網際網路並與測試電腦處於同一網域，測試電腦可透過交換器/基地台監聽待測物之封包。圖 1 為其示意圖。

圖 1 測試佈局示意圖

3. 檢測工具

3.1.檢測軟體工具

軟體	版本
beSOURCE	v 5.2.0.0
Masscan	v 1.3.2
Nmap	v 7.92
Nessus	Professional
Wireshark	v 3.6.5
HashMyFiles	v 2.38

3.2.檢測硬體工具

品名	型號
NETGEAR 8-port Gigabit Ethernet Smart Managed Pro Switch	GS308E
溫濕度錶	HTC-8

（本頁以下空白）

4. 前言

本報告之依據為經濟部標準檢驗局所公告「太陽光電變流器及監視單元資安檢測技術規範」(以下簡稱資安檢測規範)，進行檢測方法之可行性驗證，並針對目前所提之檢測方法提出改善建議，同時，藉由該檢測以確認受測之太陽光電變流器及其監視單元具有基礎資安防護能力。

依前述規範所載，變流器本體單元及監視單元之資安等級，其判準皆依表2之說明，可區分為二等，其1級低於2級，產品須先通過較低資安等級之測試，始可進行進階等級之測試。

表 2 變流器及監視單元資安等級說明

資安等級	說明	備考
1 級	防止無心之操作誤會或不成熟之攻擊行為，或防止攻擊者無足夠資源之蓄意攻擊行為。	變流器本體及監視單元之基礎資安要求。
2 級	防止蓄意且有資源之攻擊行為。	進階資安要求。

變流器及監視單元之資安要求與等級則如表3所示，第一欄為「資安構面」，包括：實體資安、系統資安及身分鑑別；第二欄為「資安要求」，係依第一欄資安構面所設計相對應之要求項目，第三欄則為「資安等級」，其係依資安要求所做之檢測標準，劃分其等級歸屬。

表 3 變流器及監視單元資安要求與資安等級一覽表

資安構面	資安要求	資安等級	
		1 級	2 級
1.1 實體資安	1.1.1 實體防護		V
1.2 系統資安	1.2.1 軟/韌體更新機制	V	V
	1.2.2 軟/韌體安全性評估		V
1.3 身分鑑別	1.3.1 人機介面身分鑑別(實體)	V	V
	1.3.2 人機介面身分鑑別(無線)	V	V
2.1 實體資安	2.1.1 實體防護		V
	2.1.2 最小實體介面要求	V	V
2.2 系統資安	2.2.1 已知脆弱性掃描	V	V
	2.2.2 軟/韌體更新機制	V	V
	2.2.3 軟/韌體安全性評估	V	V
	2.2.4 機敏資料保護	V	V
	2.2.5 惡意程式防護		V
	2.2.6 帳戶管理	V	V
	2.2.7 事件日誌	V	V
	2.2.8 事件日誌之儲存容量與效期		V
2.3 通訊資安	2.3.1 最小通訊埠要求	V	V
	2.3.2 動態資料加密保護	V	V
	2.3.3 動態資料加密保護-進階		V
	2.3.4 封包流量與指向分析	V	V
2.4 身分鑑別	2.4.1 人員使用者識別與鑑別	V	V
	2.4.2 通行碼強度(長度基礎)	V	V
	2.4.3 通行碼輸入頻次限制	V	V
	2.4.4 預設通行碼變更機制	V	V

5. 檢測項目與結果說明（以下標號依「資安檢測規範」表 2 之編號）

1.1 實體資安

1.1.1 實體防護

A. 測試說明

變流器本體應建立外殼拆除障礙或保有實體遭拆解之紀錄。

B. 測試方法

目視變流器本身之外之外殼是否為一體成形、或具實體鎖、或採防拆螺絲，以建立拆除障礙，或以一次性貼紙張貼於外殼可拆處，以保有實體遭拆解之紀錄。

C. 預期結果

目視檢查後，該變流器有建立拆除障礙，或黏貼一次性貼紙於外殼可拆處，以保有實體遭拆解之紀錄。

- 檢測結果

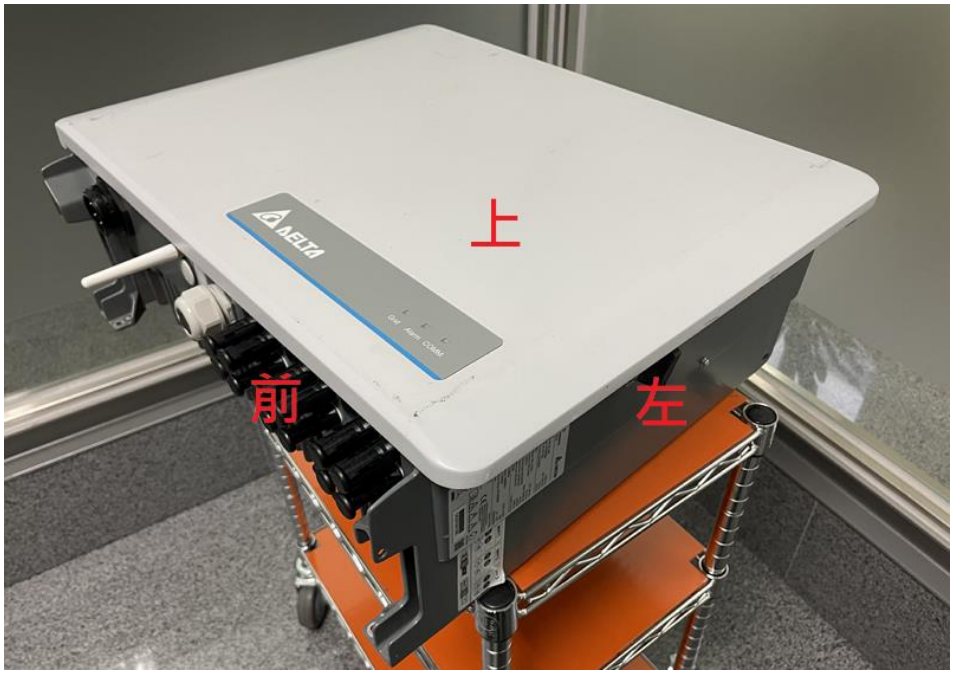
說明	結果
主型式 M30A_230 外殼以十字螺絲固定，並於可拆處之螺絲上貼有一次性貼紙，若欲拆解外殼，則須撕下或破壞該貼紙，故可保有產品外殼曾遭拆解之紀錄（見圖示 1.1.1-1）。同系列之機種亦同。 綜上所述，故判定為符合。	■符合 □不符合

（本頁以下空白）

- 檢測結果截圖說明

圖示 1.1.1-1

1. 上、前、左三面：



2. 上、後、右三面：

圖示 1.1.1-1

3. 下面：

4. 上蓋掀起便可見內部電路，故於右面環扣處貼上一次性貼紙：

5. 一次性貼紙特寫：

1.2 系統資安

1.2.1 軟/韌體更新機制

A. 測試說明

變流器之軟/韌體在更新前須驗證軟/韌體之完整性與來源可信任

B. 測試方法

1. 變流器核心功能相關之軟/韌體應有更新機制，以修補漏洞或擴充功能，廠商應提供以下項目：
   (1) 可更新之軟/韌體清單
   (2) 軟/韌體更新保護機制說明文件
   (3) 更新軟/韌體之操作程序
   (4) 可供更新之檔案
   (5) 具更新權限之帳戶
2. 依廠商提供更新檔案、具更新權限之帳戶與操作程序說明進行軟/韌體更新，應可成功更新且不會造成產品被重置為預設狀態（檢視登入帳號、系統時間、事件日誌等是否被重置），否則判為不符合。
3. 對廠商提供之軟/韌體檔案進行修改，或以其他來源之軟/韌體對該產品進行更新，應有察覺軟/韌體錯誤之機制，否則判為不合格。本體單元應能拒絕錯誤軟/韌體之更新，或顯示更新失效而回復更新前之狀態或進入待機狀態，以保護電力穩定。

C. 預期結果

1. 依廠商所提供之上述更新檔案、帳戶及操作程序進行軟/韌體更新，可成功更新且產品不會被重置為預設狀態。
2. 修改廠商提供之軟/韌體檔案，或以其他來源之軟/韌體進行更新時，本體單元可察覺軟/韌體錯誤並拒絕更新，或顯示更新失效而回復更新前之狀態或進入待機狀態。

- 檢測結果

說明	結果
1. 依廠商自我檢查表（以下稱「自檢表」）所示：同系列機種 M30A_231、M20A_220 之更新操作與保護機制皆與主型式 M30A_230 同（見附件一）。又因 COMM、DSP1、DSP2、RED 及 WIFI（屬監視單元）的韌體更新操作與保護機制皆相同，故僅以主測機種 M30A_230 之 COMM 韌體進行本測項。 2. 本系列韌體更新權限與方式： (1) 更新權限：無權限帳戶之設定，然韌體 Hex 檔僅具授權之工程人員持有，未公開予一般用戶下載；實際執行更新僅有本公司的工程人員或經銷商的安裝人員可為之。 (2) 更新方式：透過 RS485 排線連接電腦與變流器，電腦需安裝專用之韌體燒錄程式（Delta_Solar_System (DSS).exe，此軟體可由廠商官網下載）以進行更新；此外，亦可由手機 DeltaSolar App 進階權限進行更新，然僅更新介面不同，保護機制皆與前者（透過 RS485 進行更新）一致。 3. 本系列由源碼產出之韌體共有 COMM、DSP1、DSP2（ARC）、RED、WIFI 五種，變流器本體之韌體為 COMM、DSP1、DSP2（ARC）、RED 四種；WIFI 韌體則屬監視單元（見圖示 1.2.1-1）。 4. 登入帳號、系統時間、事件日誌不因更新而重置（見圖示 1.2.1-2）： 因本系列機種無登入帳號之設置，韌體更新由工程人員或經銷商安裝人員親至現場進行，若欲對變流器進行設定，則須	■符合 □不符合

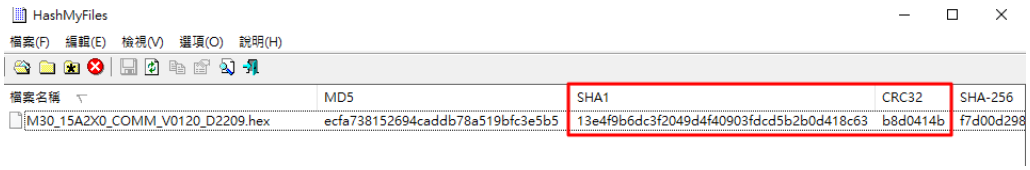
透過手機 App（DeltaSolar）及 RS485 來完成，前者身份鑑別在 App 上進行，後者無身份鑑別機制，故本體中無登入帳號因韌體更新而重置之問題；系統時間及事件日誌經檢測後亦不因更新而重置。 因產品的系統時間、事件日誌設置於變流器本體，監視單元不具備該功能，故無更新後重置之問題。 5. 韌體更新檔正確性保護機制（見圖示 1.2.1-3）： 因韌體 Hex 檔僅具授權之工程人員持有，未公開予一般用戶下載，可對韌體作初步管制。 此外，具授權之更新人員於更新前，會依「韌體更新前比對 hash 值的 SOP 說明.pdf」文件檢查韌體是否正確：先以 HashCalc 工具得出韌體的 CRC32 值，再與廠商所提供之 CRC32 值比對，兩者一致方進行更新。 綜上所述，故判定為符合。	

- 檢測結果截圖說明

圖示 1.2.1-1

擷取韌體 SHA1 及 CRC32 值：

1. COMM 韌體
   版本：V1.20，檔名：M30_15A2X0_COMM_V0120_D2209.HEX
   CRC32：b8d0414b
   SHA1：13e4f9b6dc3f2049d4f40903fdcd5b2b0d418c63



圖示 1.2.1-1

比對自檢表所附該韌體之 CRC32 值，兩者一致。

COMM.：V1.20

M30_15A2X0_COMM_V0120_D2209.HEX

Hash CRC32: b8d0414b

2. DSP1 韌體

版本：V1.16，檔名：M30_15A2X0_DSP1_V0116_D2209_DBV7.HEX

CRC32：27dc3641

SHA1：82eecf26268578191624c26110c71a1e72b7c01e

比對自檢表所附該韌體之 CRC32 值，兩者一致。

DSP1：V1.16

M30_15A2X0_DSP1_V0116_D2209_DBV7.HEX

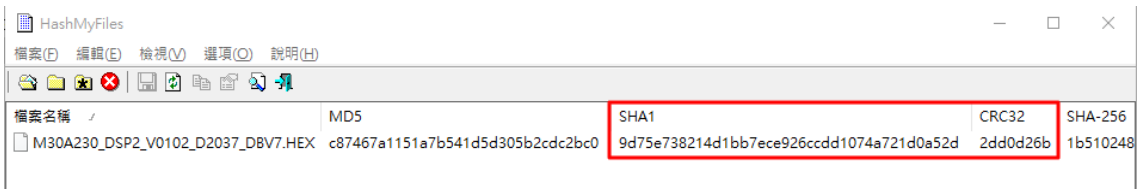
Hash CRC32: 27dc3641

3. DSP2（ARC）韌體

版本：V1.02，檔名：M30A230_DSP2_V0102_D2037_DBV7.HEX

CRC32：2dd0d26b

SHA1：9d75e738214d1bb7ece926ccdd1074a721d0a52d



圖示 1.2.1-1

比對自檢表所附該韌體之 CRC32 值，兩者一致。

DSP2：V1.02

M30A230_DSP2_V0102_D2037_DBV7.HEX

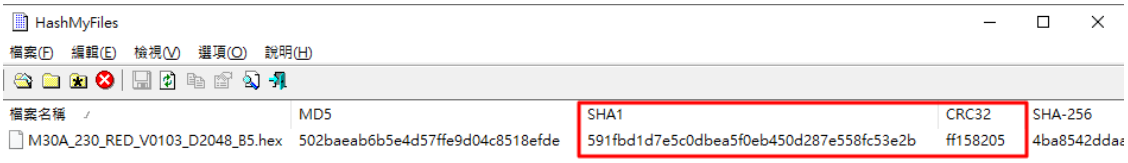
Hash CRC32: 2dd0d26b

4. RED 韌體

版本：V1.03，檔名：M30A_230_RED_V0103_D2048_B5.HEX

CRC32：ff158205

SHA1：591fbd1d7e5c0dbea5f0eb450d287e558fc53e2b



比對自檢表所附該韌體之 CRC32 值，兩者一致。

RED：V1.03

M30A_230_RED_V0103_D2048_B5.HEX

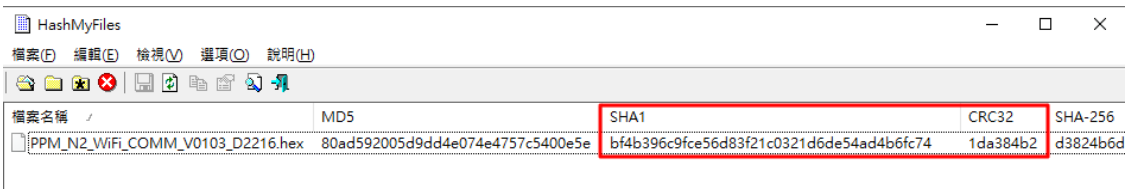
Hash CRC32: ff158205

5. WIFI 韌體（屬監視單元）

版本：V1.03，檔名：PPM_N2_WiFi_COMM_V0103_D2216.HEX

CRC32：1da384b2

SHA1：bf4b396c9fce56d83f21c0321d6de54ad4b6fc74



圖示 1.2.1-1

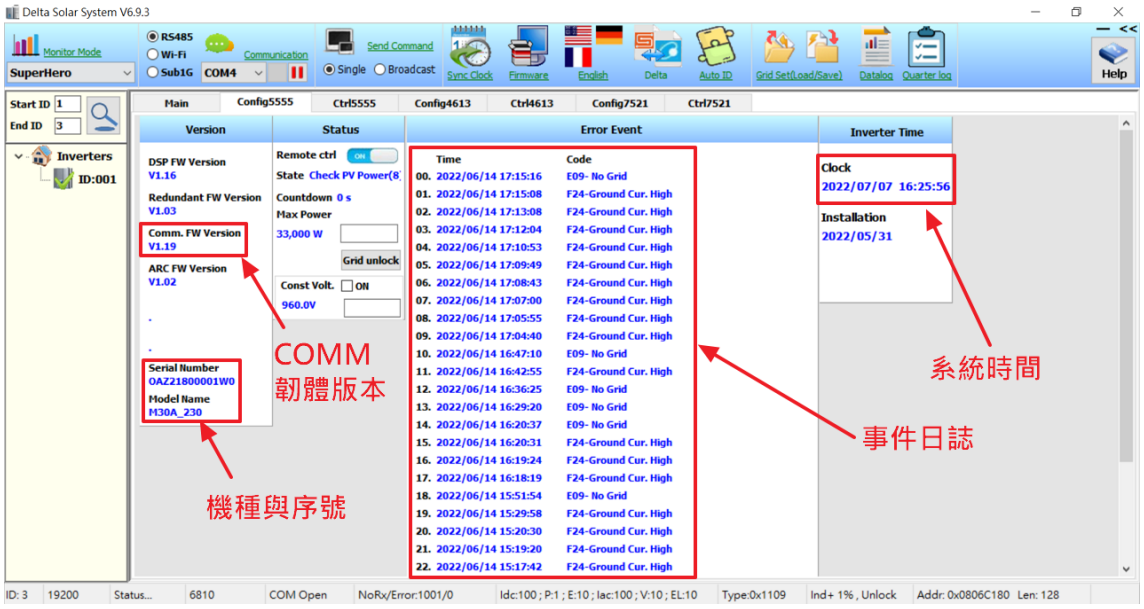
比對自檢表所附該韌體之 CRC32 值，兩者一致。

更新用之版本：V1.03
PPM_N2_WiFi_COMM_V0103_D2216.HEX
Hash CRC32: 1da384b2

圖示 1.2.1-2

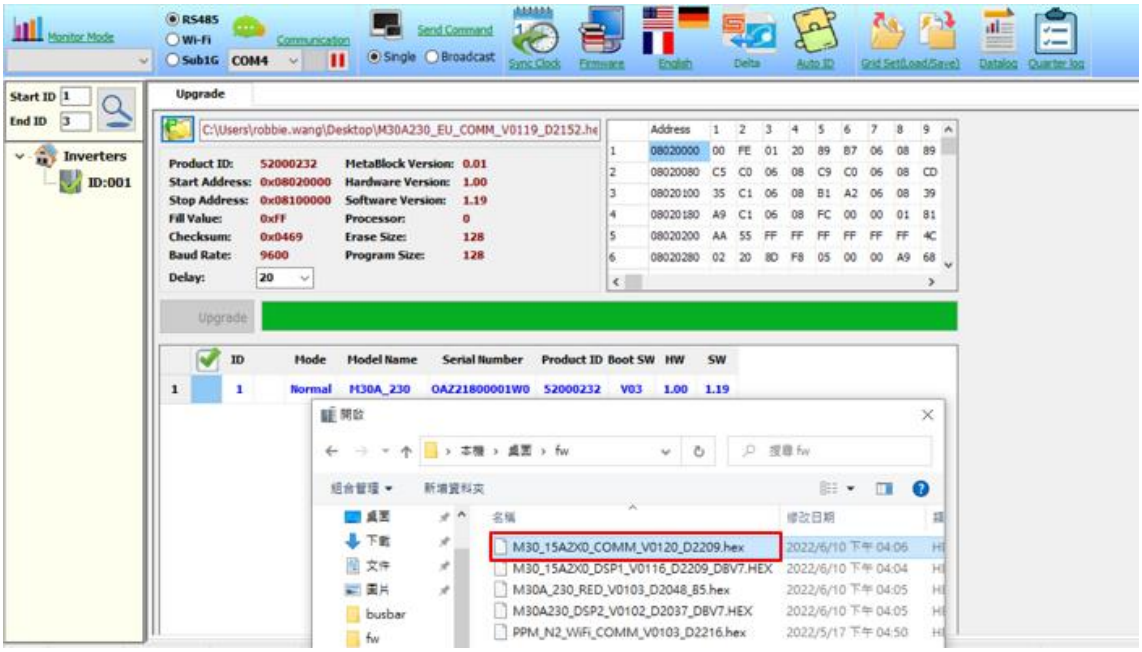
本系列機種無設置登入帳號；系統時間、事件日誌不因更新而重置：

1. 開啟燒錄程式 Delta_Solar_System (DSS).exe，檢視 M30A_230 變流器更新前之韌體版本、系統時間及事件日誌，其版本為 V1.19 時間為 2022/07/07 16:25:56，事件日誌顯示 22 筆紀錄。

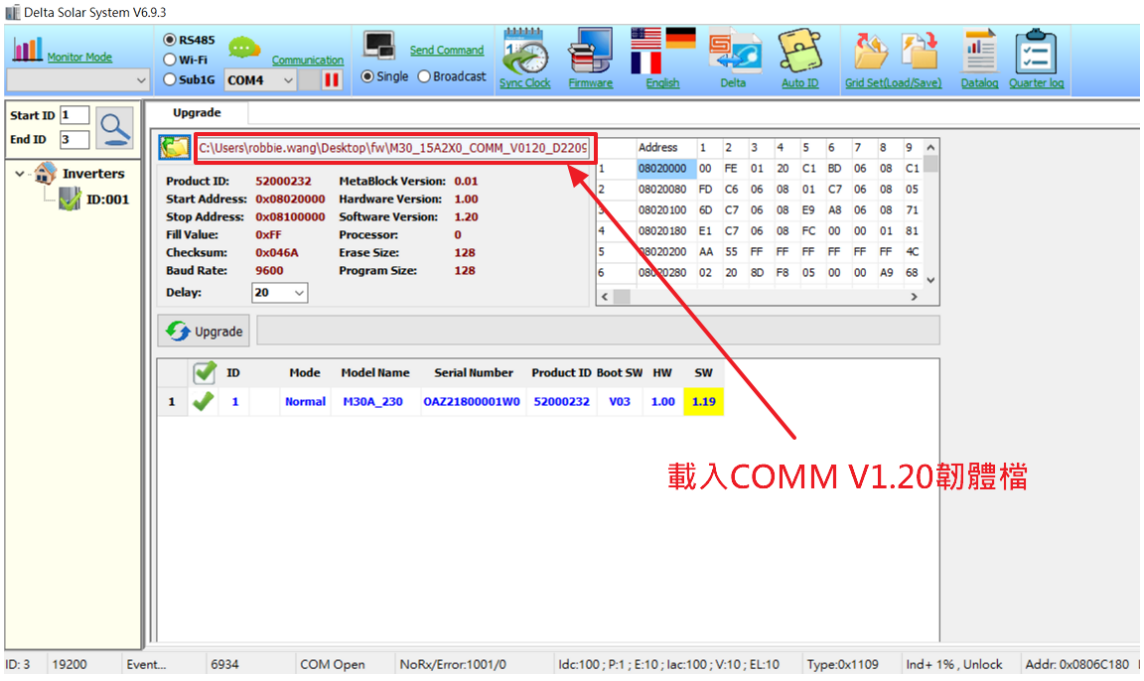


圖示 1.2.1-2

2. 選取欲更新之韌體檔——M30_15A2X0_COMM_V0120_D2209.HEX：

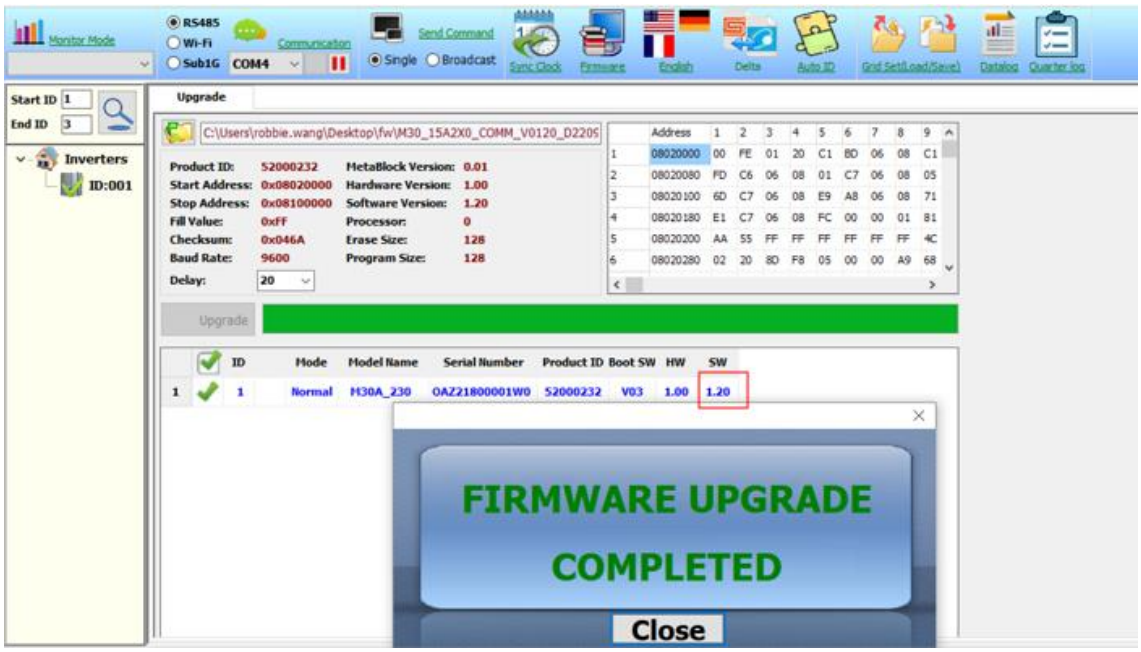


3. 韌體載入成功：

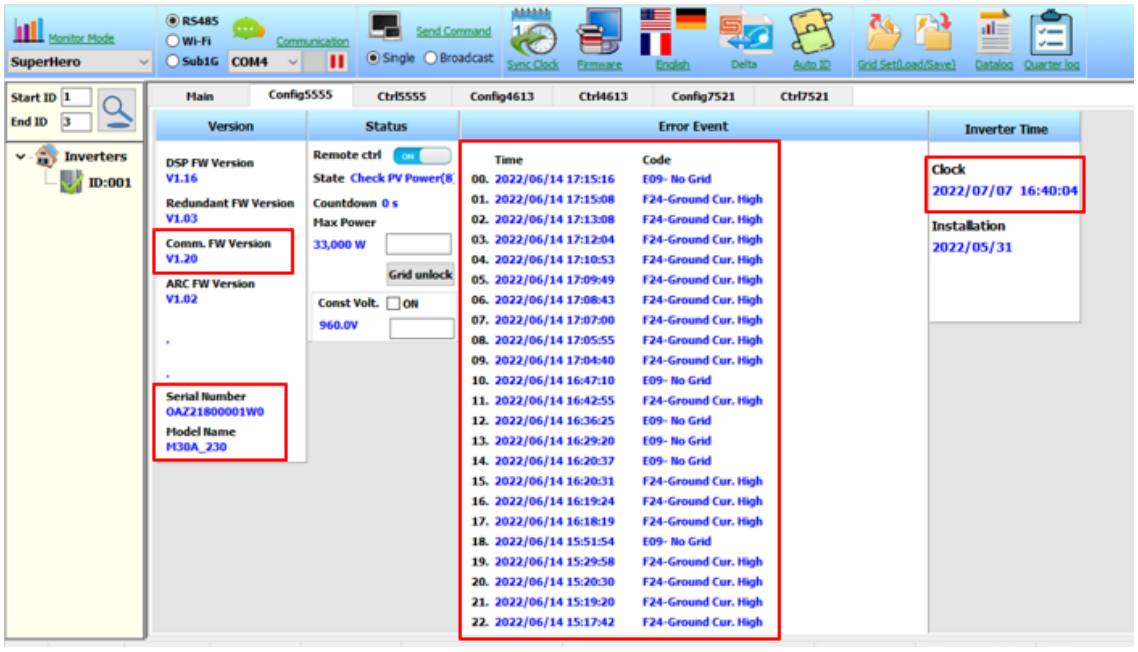


圖示 1.2.1-2

4. 完成韌體更新：



5. 檢視更新後之韌體版本已變更為 V1.20，而系統時間與事件日誌皆未被重置為預設狀態：



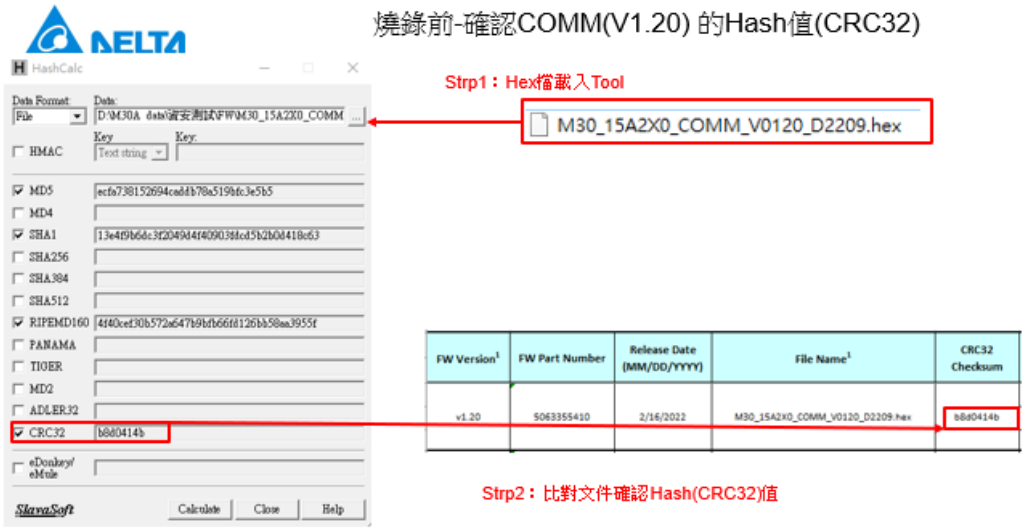
圖示 1.2.1-3

韌體更新檔完整性保護機制：

更新前，被授權更新之安裝人員會依「韌體更新前比對 hash 值的 SOP 說明.pdf」文件所述，比對韌體 CRC32 值以確保其完整性。

依該文件之指引：

1. 公司會提供欲更新韌體之 CRC32 值給安裝人員。
2. 韌體更新前，安裝人員須以 HashCalc 工具確認韌體 CRC32 值是否一致，若一致則進行更新，反之則否。如以 COMM 韌體為例：



1.2.2 軟/韌體安全性評估

A. 測試說明

變流器之軟/韌體程式碼應進行靜態分析以確認資安弱點。

B. 測試方法

1. 廠商應提供於 1.2.1 測試項目中進行軟/韌體更新之程式源碼（source code）作為安全性評估之標的。
2. 對標的檔案進行靜態程式碼弱點分析。分析工具應可識別

共同弱點（CWE）或共同脆弱性（CVE）並比對弱點或脆弱性評分系統（CWSS/CVSS）以進行等級判定。

3. 若測得具共同弱點/脆弱性（CWE/CVE）編號之漏洞，且其 CWSS/CVSS 分數大於等於 7（或嚴重等級為 High 或 Critical 者），廠商應能提供合理管控措施並說明之，否則本項不符合。

C. 預期結果

1. 以分析工具測檢測後，無 CWE/CVE 編號之漏洞；若有，則其 CWSS/CVSS 分數小於 7（或等級非 High 或 Critical）。
2. CWSS/CVSS 分數大於等於 7（或嚴重等級為 High 或 Critical）者，廠商能提供合理管控措施並說明之。

- 檢測結果

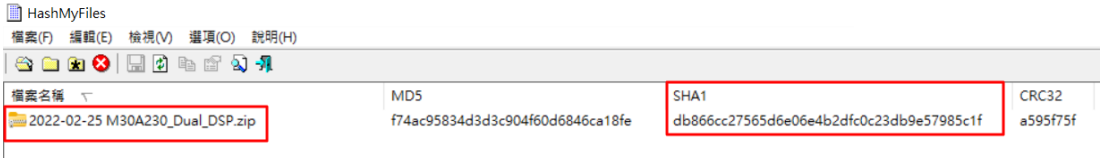
說明	結果
1. 本系列之變流器本體韌體源碼共有 COMM、DSP1、DSP2（ARC）及 RED 四種，其中，DSP1 與 DSP2 的源碼置於同一包壓縮檔中，故共有 COMM、DSP 及 RED 三包源碼（見圖示 1.2.2-1）。 2. 使用源碼掃描軟體 beSOURCE（v 5.2.0.0）對 COMM、DSP 及 RED 韌體源碼進行掃描後，其結果皆無 Critical 及 Rec.-High 之漏洞，故判定為符合（見圖示 1.2.2-2）。	■符合 □不符合

- 檢測結果截圖說明

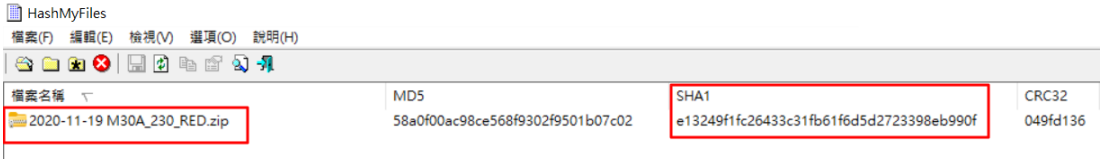
圖示 1.2.2-1
1. COMM V1.20 韌體源碼壓縮檔之 SHA1 值為： a0448ecdee4aa11c8ff8782f7570dbe1a5acb350

圖示 1.2.2-1

2. DSP 韌體源碼壓縮檔（包含 DSP1 V1.16 與 DSP2 V1.02）之 SHA1 值為：db866cc27565d6e06e4b2dfc0c23db9e57985c1f



3. RED V1.03 韌體源碼壓縮檔之 SHA1 值為：e13249f1fc26433c31fb61f6d5d2723398eb990f



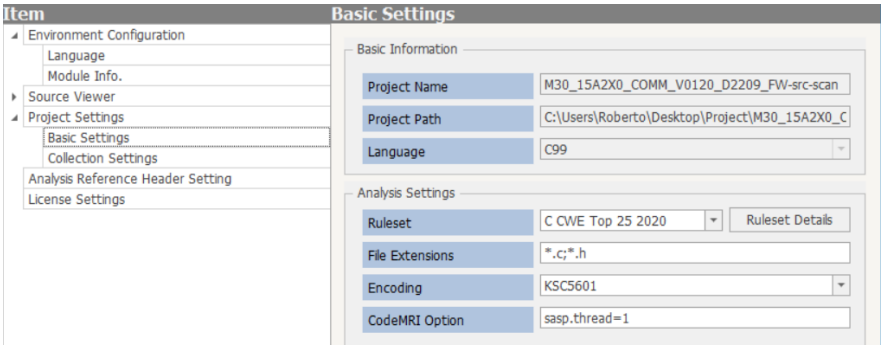
圖示 1.2.2-2

1. beSOURCE 掃描 COMM V1.20 源碼所採用之設定：

   Language：C99

   Ruleset：C CWE Top 25 2020

   File Extensions：*.c;*.h



圖示 1.2.2-2

COMM 源碼掃描結果無 Critical 及 Rec.-High 之漏洞：

Report for Analysis Results

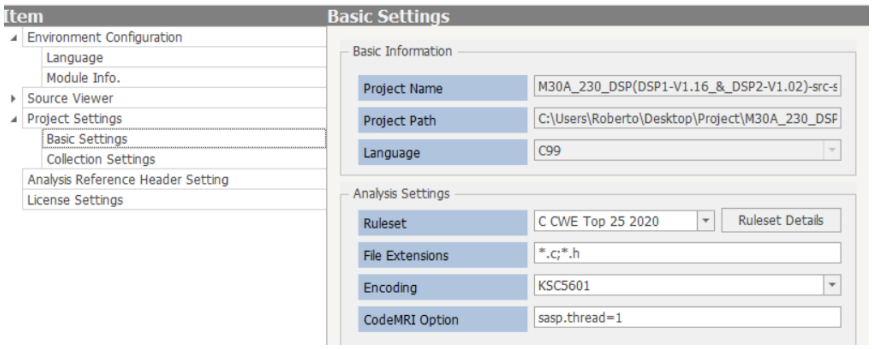
ProjectName: M30_15A2X0_COMM_V0120_D2209_FW-src-scan **Language:** C99

Ruleset: C CWE Top 25 2020 **Analysis DateTime:** 2022.07.06 11:52:12

Summary

		Detected Files by Priority		Detected Rules by Priority	
File Count :	391	Critical	0	Critical	0
LOC :	135	Rec.-High	0	Rec.-High	0
Detected Files :	0	Rec.-Middle	0	Rec.-Middle	0
Detected Rules :	0	Rec.-Low	0	Rec.-Low	0
Detected Rules Count:	0	Info.	0	Info.	0

2. beSOURCE 掃描 DSP（包含 DSP1 V1.16 與 DSP2 V1.02）源碼所採用之設定同於 COMM V1.20：



源碼掃描結果無 Critical 及 Rec.-High 之漏洞：

Report for Analysis Results

ProjectName: M30A_230_DSP(DSP1-V1.16_&_DSP2-V1.02)-src-scan **Language:** C99

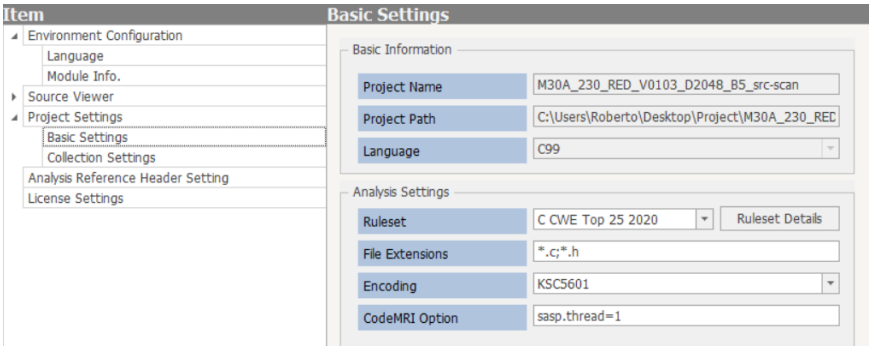
Ruleset: C CWE Top 25 2020 **Analysis DateTime:** 2022.06.16 13:45:19

Summary

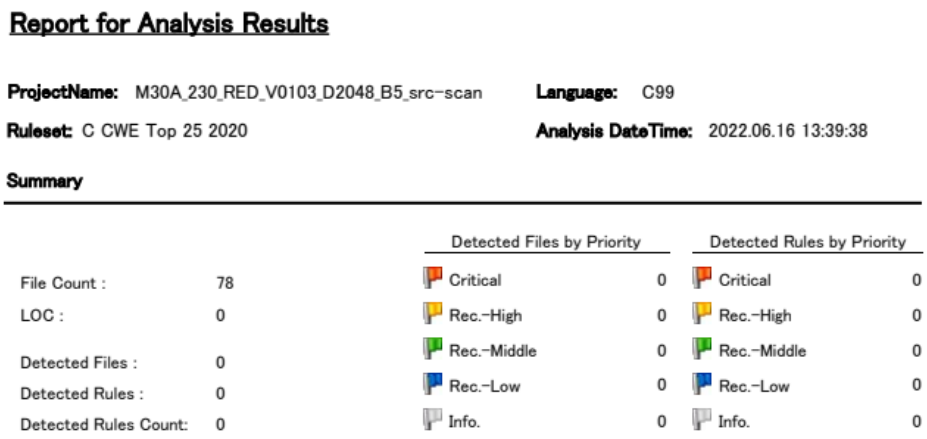
		Detected Files by Priority		Detected Rules by Priority	
File Count :	124	Critical	0	Critical	0
LOC :	66,040	Rec.-High	0	Rec.-High	0
Detected Files :	10	Rec.-Middle	0	Rec.-Middle	0
Detected Rules :	890	Rec.-Low	0	Rec.-Low	0
Detected Rules Count:	2	Info.	10	Info.	890

圖示 1.2.2-2

3. beSOURCE 掃描 RED 源碼所採用之設定同於 COMM V1.20：



RED 源碼掃描結果無 Critical 及 Rec.-High 之漏洞：



1.3 身份鑑別

1.3.1 人機介面身份鑑別（實體）

A. 測試說明

透過實體人機介面（如顯示面板與按鍵）存取/操作變流器，應有權限管理與鑑別機制。

B. 測試方法

1. 未採用實體人機介面之產品，或實體人機介面僅具資料查詢與顯示功能，本項可申明為不適用。
2. 廠商應提供實體人機介面鑑別機制、存取方式與操作權限之說明，並提供可通過鑑別之鑑別符（如通行碼、感應磁

扣等)。

3. 以步驟2提供之鑑別符，應能通過鑑別並存取裝置，確認操作權限與廠商說明相符，則本項符合。

4. 若未經鑑別可以對變流器本體進行電力相關參數變更（如改變輸出電壓、頻率等)，則本測項不符合。為確保人員或產品安全相關之切斷開關則不在此限。

C. 預期結果

以廠商提供之鑑別符可通過鑑別並存取裝置，且操作權限與廠商說明相符。

- 檢測結果

說明	結果
依自檢表（見附件一）宣告「本系列產品之實體人機介面僅有燈號」，故不適用本測項。 經檢視後，其結果與廠商所述一致（見圖示 1.3.1-1)，故判定為不適用。	□符合 □不符合 ■不適用

- 檢測結果截圖說明

圖示 1.3.1-1

1.3.2 人機介面身份鑑別（無線）

A. 測試說明

對透過無線之人機介面（如透過藍芽）存取/操作變流器，應有權限管理與鑑別機制。

B. 測試方法

1. 未採用無線人機介面之產品，或無線人機介面僅具資料查詢與顯示功能，則此項可申明為不適用。
2. 廠商應提供無線人機介面鑑別機制、存取方式與操作權限之說明，並提供可通過鑑別之鑑別符。
3. 以步驟 2 提供之鑑別符，應能通過鑑別並存取裝置，確認操作權限與廠商說明相符，則本項符合。
4. 若此無線介面採預設之通行碼作為鑑別符，宜有強制使用者更新通行碼之機制，若否，則此預設通行碼不得為：
   (1) 可公開取得之資訊（如登載於產品說明書內）
   (2) 公認之弱通行碼形式，如：與帳號相同、採常見預設通行碼或單詞（ex. admin, root, password）、重複字元（ex. kkkkk）、低於 8 碼之純數字組合、鍵盤按鍵順序組合（ex. qwert）等。

C. 預期結果

1. 以廠商所提供之鑑別符，能通過鑑別並存取裝置，且操作權限與廠商說明相符。
2. 若此無線介面採預設之通行碼作為鑑別符，則有強制使用者更新通行碼之機制；若否，則預設通行碼非為(1)可公開取得之資訊，或(2)公認之弱通行碼形式。

- 檢測結果

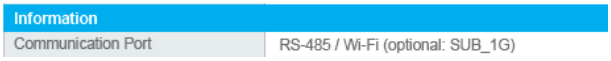
說明	結果
1. 依自檢表之宣告，本系列產品具備 WIFI 及 SUB_1G（選配）無線通訊功能。SUB_1G 須選配廠商專屬之天線，並經由廠商專屬之 DC（Data Collector，屬監視單元，具 WIFI 通	□符合 □不符合 ■不適用

訊介面以連接網際網路）結合 N1（SUB_1G 通訊模組，與變流器 SUB_1G 建立連線，並傳輸變流器與 DC 間之數據），方可實現無線通訊之功能。型錄所載規格亦同（見圖示 1.3.2-1）。 2. 因 SUB_1G 人機介面設計於 App（DeltaSolar）上（見圖示 1.3.2-2），而 WIFI 模組屬內嵌式監視單元，因此對於變流器本體而言，本測項不適用。	

- 檢測結果截圖說明

圖示 1.3.2-1

產品型錄所載通訊埠資訊：



圖示 1.3.2-2

SUB_1G 人機介面：

將變流器 SUB_1G 與 DC 的 N1 模組連接，再以手機 WIFI 連入 DC，並透過 App——DeltaSolar 與設備建立連線。若欲對變流器進行設定，則須先至設定頁面（Grid Setting）通過身分鑑別後，方可為之。

2.1 實體資安

2.1.1 實體防護

A. 測試說明

監視單元應建立外殼拆除障礙。

B. 測試方法

目視監視單元之外殼，應一體成形、或具實體鎖或設計於可上鎖之箱體內、或採防拆螺絲搭配一次性貼紙，以建立拆除障礙。

C. 預期結果

目視檢查後，該變流器有建立拆除障礙，或黏貼一次性貼紙於外殼可拆處，以保有實體遭拆解之紀錄。

- 檢測結果

說明	結果
主型式 M30A_230 之內嵌式監視單元（WIFI 通訊模組）外殼處，以星形螺絲固定，並於可拆處上貼有一次性貼紙，若欲拆解，則須撕下或破壞該貼紙，故可保有產品外殼曾遭拆解之紀錄（見圖示 2.1.1-1）。同系列之機種亦同。 綜上所述，故判定為符合。	■符合 □不符合

- 檢測結果截圖說明

圖示 2.1.1-1

1. 監視單元（WIFI 通訊模組）外殼處，使用星形螺絲搭配一次性貼紙：

2. 星形螺絲與一次性貼紙特寫：

2.1.2 最小實體介面要求

A. 測試說明

應將監視單元上非必要之實體介面（如 USB 埠、RJ45 埠、SD Card 插槽等）移除或預設為關閉，以減少可能被攻擊之途徑。

B. 測試方法

1. 廠商提供文件說明實體介面之目的及相關保護措施。目視產品外觀並清點實體介面應與廠商說明文件相符，否則此項判為不符合。

2. 如存有非必要之實體介面未移除，則應預設關閉或採實體保護，否則此項判為不符合。

C. 預期結果

1. 目視檢查產品外觀及清點實體介面後，其外觀與介面與廠商說明文件相符。
2. 如存有非必要之實體介面未移除，該介面預設為關閉或採實體保護之。

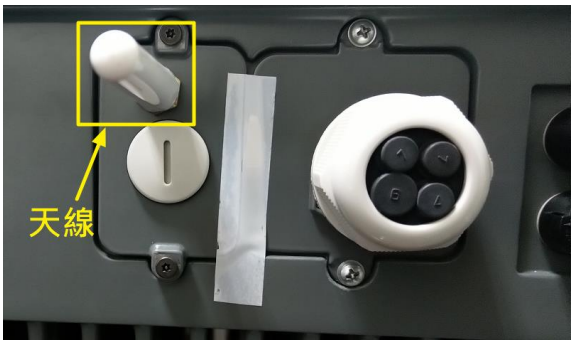
- 檢測結果

說明	結果
依自檢表所宣告：「設備僅有 WIFI 天線，餘無外露之實體介面」。 檢視其介面，確實與廠商所述一致（見圖示 2.1.2-1），故判定為符合。	■符合 □不符合

- 檢測結果截圖說明

圖示 2.1.2-1

WIFI 天線介面：



2.2 系統資安

2.2.1 已知脆弱性掃描

A. 測試說明

監視單元不應存在風險等級較高之已知脆弱性。

B. 測試方法

1. 使用弱點識別工具對產品進行弱點掃描，脆弱性識別應依共同脆弱性評分系統（CVSS）進行判定。
2. 若測得共同脆弱性及暴露（CVE）編號之漏洞，且其 CVSS 分數大於等於 7（或嚴重等級為 High 或 Critical 者）則本項不符合。
3. 若帶有中等級之脆弱性，廠商應能提供合理管控措施，否則本項不符合。

C. 預期結果

1. 弱點識別工具對產品進行弱點掃描後，無 CVE 編號之漏洞；若有，則其 CVSS 分數小於 7（或等級非 High 或 Critical）。
2. 帶有中等級之脆弱性者，廠商能提供合理管控措施並說明之。

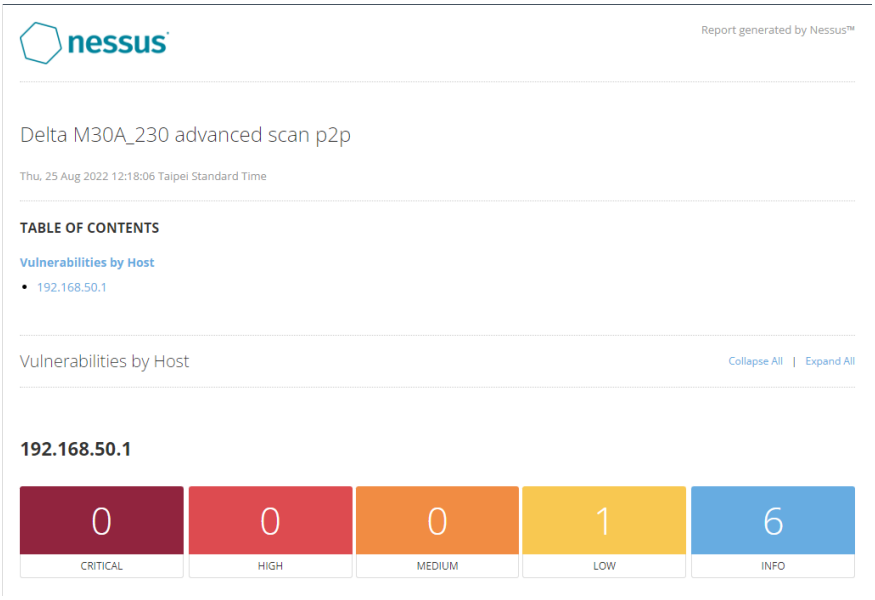
- 檢測結果

說明	結果
以 Nessus professional 之 Advanced Scan 對主型式 M30A_230 之系統進行掃描，其結果： 1. 於 P2P mode 下掃描：Low 計 1 處，Info 計 6 處。 2. 於 Client mode 下掃描： Info 計 6 處。 綜上所述，無 Critical 或 High 之漏洞，故判定為符合。	■符合 □不符合

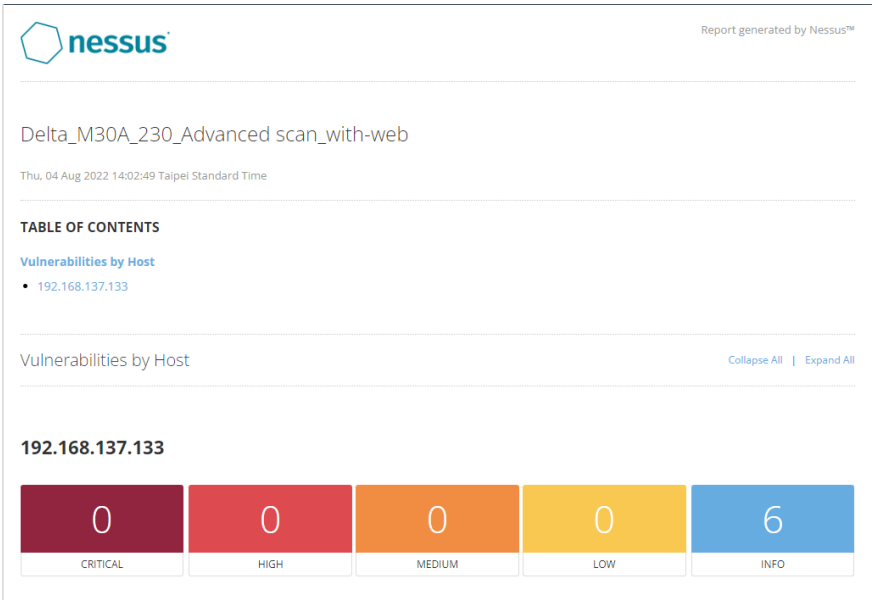
- 檢測結果截圖說明

圖示 2.2.1-1

1. 於 P2P mode 下之掃描結果：



2. 於 Client mode 下之掃描結果：



2.2.2 軟/韌體更新機制

A. 測試說明

監視單元之軟/韌體在更新前須驗證軟/韌體之完整性與來源可信任

B. 測試方法

1. 監視單元核心功能相關之軟/韌體應有更新機制，以修補漏洞或擴充功能，廠商應提供以下項目：
   (1) 可更新之軟/韌體清單
   (2) 軟/韌體更新保護機制說明文件
   (3) 更新軟/韌體之操作程序
   (4) 可供更新之檔案
   (5) 具更新權限之帳戶
2. 依廠商提供更新檔案、具更新權限之帳戶與操作程序說明進行軟/韌體更新，應可成功更新且不會造成產品被重置為預設狀態（檢視登入帳號、系統時間、事件日誌等是否被重置），否則判為不符合。
3. 對廠商提供之軟/韌體檔案進行修改，或以其他來源之軟/韌體對該產品進行更新，應有察覺軟/韌體錯誤之機制，否則判為不合格。

C. 預期結果

1. 依廠商所提供之上述更新檔案、帳戶及操作程序進行軟/韌體更新，可成功更新且產品不會被重置為預設狀態。
2. 修改廠商提供之軟/韌體檔案，或以其他來源之軟/韌體進行更新時，本體單元可察覺軟/韌體錯誤並拒絕更新，或顯示更新失效而回復更新前之狀態或進入待機狀態。

- 檢測結果

說明	結果
因同系列機種 M30A_231、M20A_220 之更新操作與保護機制皆與主型式 M30A_230 同。又 COMM、DSP1、DSP2、RED 與 WIFI 韌體更新操作與保護機制皆相同，依測項 1.2.1 之檢測結	■符合 □不符合

果，故判定為符合。	

2.2.3 軟/韌體安全性評估

A. 測試說明

監視單元之軟/韌體程式碼應進行靜態分析以確認資安弱點。

B. 測試方法

1. 廠商應提供於 2.2.2 測試項目中進行軟/韌體更新之檔案程式源碼（source code）作為安全性評估之標的。
2. 對標的檔案進行靜態程式碼弱點分析。分析工具應可識別共同弱點（CWE）或共同脆弱性（CVE）並比對弱點或脆弱性評分系統（CWSS/CVSS）以進行等級判定。
3. 若測得具共同弱點/脆弱性（CWE/CVE）編號之漏洞，且其 CWSS/CVSS 分數大於等於 7（或嚴重等級為 High 或 Critical 者），廠商應能提供合理管控措施並說明之，否則本項不符合。

C. 預期結果

1. 以分析工具測檢測後，無 CWE/CVE 編號之漏洞；若有，則其 CWSS/CVSS 分數小於 7（或等級非 High 或 Critical）。
2. CWSS/CVSS 分數大於等於 7（或嚴重等級為 High 或 Critical）者，廠商能提供合理管控措施並說明之。

- 檢測結果

說明	結果
1. 本系列之機種僅有一包 WIFI 韌體源碼，其版本號為 V1.03（見圖示 2.2.3-1）。 2. 使用源碼掃描軟體 beSOURCE（v 5.2.0.0）對該韌體源碼進行掃描後，其結果皆無 Critical 及 Rec.-High 之漏洞，故判定	■符合 □不符合

為符合（見圖示 2.2.3-2）。	

- 檢測結果截圖說明

圖示 2.2.3-1

擷取 WIFI V1.03 韌體源碼壓縮檔之 SHA1 值：

SHA1：b09cbc575df640ba64d2ed6bf42bbc45c26fddf3

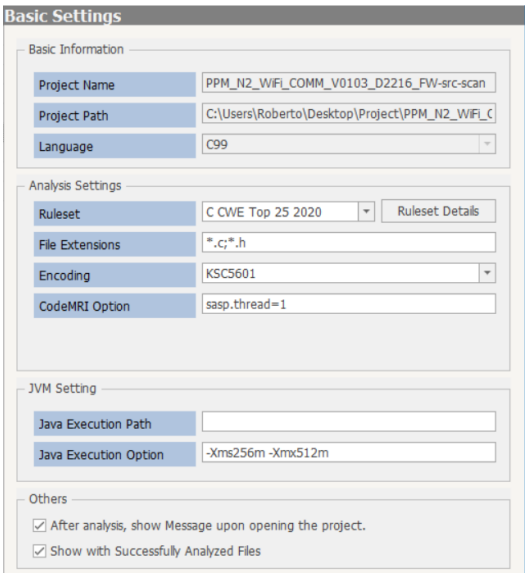
圖示 2.2.3-2

beSOURCE 掃描 WIFI V1.03 源碼所採用之設定：

Language：C99

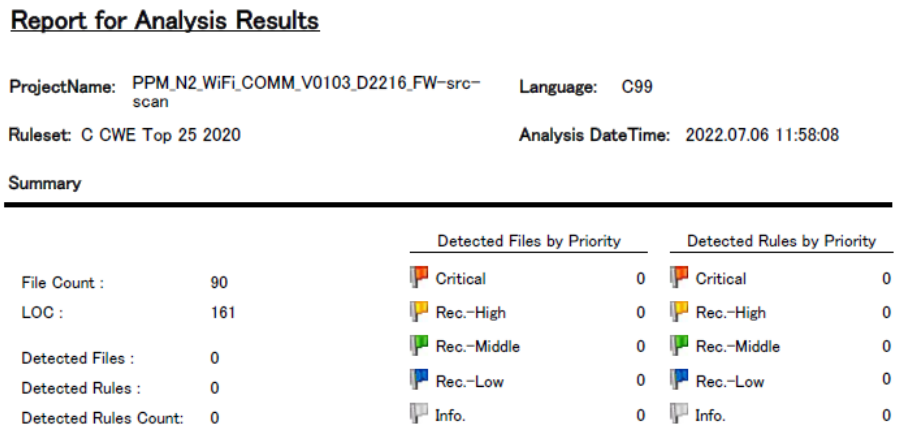
Ruleset：C CWE Top 25 2020

File Extensions：*.c;*.h



圖示 2.2.3-2

WIFI 源碼掃描結果無 Critical 及 Rec.-High 之漏洞：



Report for Analysis Results

ProjectName: PPM_N2_WiFi_COMM_V0103_D2216_FW-src-scan **Language:** C99

Ruleset: C CWE Top 25 2020 **Analysis DateTime:** 2022.07.06 11:58:08

Summary

File Count :	90
LOC :	161
Detected Files :	0
Detected Rules :	0
Detected Rules Count:	0

Detected Files by Priority		Detected Rules by Priority	
Critical	0	Critical	0
Rec.-High	0	Rec.-High	0
Rec.-Middle	0	Rec.-Middle	0
Rec.-Low	0	Rec.-Low	0
Info.	0	Info.	0

2.2.4 機敏資料保護

A. 測試說明

監視單元儲存之機敏資料應受到保護。

B. 測試方法

1. 機敏資料包括但不限於身分鑑別資訊（如使用者帳號、通行碼）及含有使用者隱私之資料，廠商應提供自定義之機敏資料說明。若監視單元內無儲存機敏資料，則本項可聲明為不適用。
2. 廠商應說明對機敏資料之保護方式，如將機敏資料加密，或置於需要特殊權限方能存取之資料路徑。
3. 驗證廠商之保護說明：以沒有特殊權限的一般帳戶登入並嘗試存取機敏資料，如未能成功存取，則本項符合。

C. 預期結果

以沒有特殊權限的一般帳戶登入後，未能成功存取機敏資料。

- 檢測結果

說明	結果
廠商於自檢表宣告：「本系列機種皆無儲存機敏資料」。 依測項 1.2.1，經由 RS485 介面連接 M30A_230，其本體及監視單元皆無登入帳號之設計。 由上述可知，監視單元無儲存機敏資料，與廠商宣告一致，故本測項不適用。	□符合 □不符合 ■不適用

2.2.5惡意程式防護

A. 測試說明

監視單元應防止來源不明、未授權或已知含有惡意程式的軟/韌體被安裝或被執行。

B. 測試方法

1. 若監視單元為嵌入式裝置則通過測試項目 2.2.2、2.2.3，此項次即符合。
2. 若監視單元為主機裝置，除第 1 條所述之通過要件外，應採取合宜措施防範惡意程式碼（例：針對病毒、蠕蟲、特洛伊木馬程式及間諜軟體）並提供說明，以書面審查判定本項是否符合。

C. 預期結果

1. 監視單元為嵌入式裝置者，通過測試項目 2.2.2、2.2.3。
2. 監視單元為主機裝置者，除通過測試項目 2.2.2、2.2.3 外，對惡意程式碼有合宜之防範措施，並提供相關之說明。

- 檢測結果

說明	結果
廠商宣告：「本監視單元為嵌入式系統，無獨立作業系統在內。」 以 nmap 指令對監視單元之作業系統進行推測，其結果與廠商宣告一致（見圖示 2.2.5-1），故判定為符合。	■符合 □不符合

- 檢測結果截圖說明

圖示 2.2.5-1

以 nmap -O 指令掃描監視單元，其推測之作業系統多為嵌入式系統。

```
PS C:\Windows\system32> nmap -O 192.168.50.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-25 13:29 台北標準時間
Nmap scan report for 192.168.50.1
Host is up (0.0057s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
5001/tcp open  commplex-link
MAC Address: 80:C9:55:12:55:A8 (Redpine Signals)
Device type: storage-misc|phone|VoIP adapter
Running (JUST GUESSING): Apple embedded (90%), Nokia Symbian OS (89%), Cisco embedded (88%),
Sony Ericsson embedded (86%), Linksys embedded (85%)
OS CPE: cpe:/o:nokia:symbian_os cpe:/h:cisco:ata_188_voip_gateway cpe:/h:sonyericsson:w705 cp
e:/h:sonyericsson:w715
Aggressive OS guesses: Apple Time Capsule NAS device (90%), Nokia 3600i mobile phone (89%), C
isco ATA 188 VoIP adapter (88%), Sony Ericsson W705 or W715 Walkman mobile phone (86%), Links
ys PAP2T VoIP router (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.13 seconds
```

2.2.6 帳戶管理

A. 測試監視單元應提供人員使用者至少二階層（如管理員及一般使用者）以上之存取權限，以利分級管理，或經由管理系統之支援達成此項要求。

B. 測試方法

1. 廠商應就所有人員使用者可存取產品之途徑提供說明。

2. 基於使用者角色之差異，應至少須有二階層以上之存取權限，且應符合最少權限原則。

3. 人員使用者可存取監視單元之介面可能存在於本地端或遠端（管理系統），帳戶管理要求可於任一端實踐之。

4. 廠商應就步驟 1～3 所述提出書面說明，以審閱判斷是否符合要求。

5. 廠商應提供測試用帳戶。登入較低權限之帳號，並嘗試存取需較高權限之資料或需較高權限之操作。若能成功登入且無法進行存取需較高權限之資料，或無法進行需較高權限之操作，則本項符合。

6. 廠商得申明「最低權限使用者」（如僅具閱覽展示資訊之權限），此等使用者得採用較弱之識別與鑑別程序。惟此等「最低權限使用者」不應授予存取 2.2.4 所列之機敏資料（除該使用者本身之帳號或隱私資訊）之權限、不應授予如 1.2.1 及 2.2.2 所述進行軟/韌體更新之權限、不應授予於遠端控制變流器之行為之權限，且不應授予修改變流器電力相關參數之權限。

C. 預期結果

1. 廠商就步驟 1～3 所述而提出之書面說明符合要求。其包含：
   (1) 所有人員使用者可存取產品之途徑。
   (2) 角色之差異至少有二階層以上之存取權限，且符合最少權限原則。
   (3) 人員使用者可存取監視單元之介面，不論存在於本地端或遠端（管理系統），帳戶管理皆可於任一端實踐之。
2. 登入較低權限之帳號，能成功登入且無法進行存取需較高權限之資料，或無法進行需較高權限之操作。
3. 廠商若有申明「最低權限使用者」，其不被授予：
   (1) 存取 2.2.4 所列之機敏資料（除該使用者本身之帳號或隱私資訊）之權限
   (2) 如 1.2.1 及 2.2.2 所述進行軟/韌體更新之權限。
   (3) 於遠端控制變流器之行為之權限
   (4) 修改變流器電力相關參數之權限。

- 檢測結果

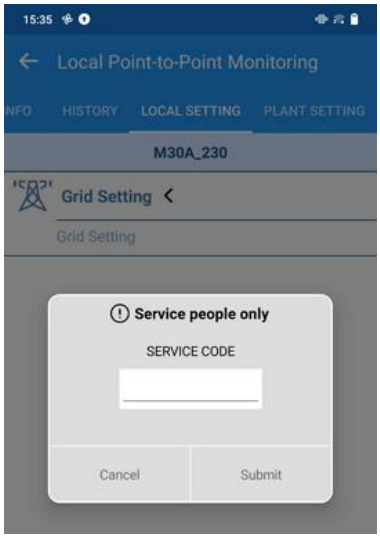
說明	結果
廠商自檢表宣告存取監視單元帳戶類別有： 1. DeltaSolar App 介面： (1) Local Monitoring：P2P mode 及 Client mode A. 一般用戶：僅能查看發電或設備異常資訊 B. 進階用戶：可透過經授權之密碼做併網參數設定（Grid setting）及韌體更新（FW upgrade） (2) Remote Monitoring 只有一般用戶，僅有查詢或瀏覽之權限。 2. 監視單元 WEB 介面：僅於 P2P mode 下顯示 此為 WIFI 晶片商（Redpine Signals）預設自帶的 WEB 管理介面；此介面無帳號及身分鑑別機制，然僅在 PSP mode 下可透過預設 80 port 進入，一旦進入 Client mode（可連上 internet）便關閉。 3. 太陽能雲 WEB 介面： 只有一般用戶，除變更其帳戶之登入密碼外，僅可瀏覽發電或設備異常資訊，為最低權限使用者。 經檢測後，DeltaSolar App（見圖示 2.2.6-1）、監視單元 WEB（見圖示 2.2.6-2）及太陽能雲 WEB（見圖示 2.2.6-3）其帳戶權限設計合於規範要求，故判定為符合。	■符合 □不符合

- 檢測結果截圖說明

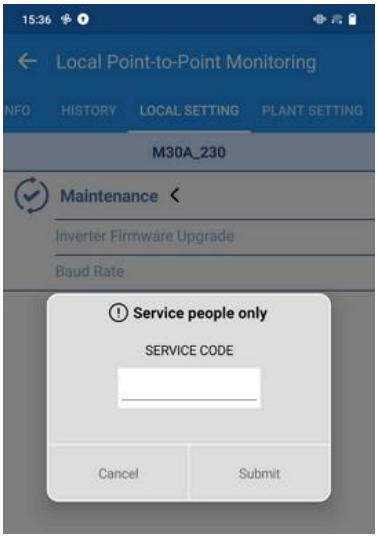
圖示 2.2.6-1
DeltaSolar App 介面 1. 本地監控（Local Monitoring）：手機透過 WIFI 連接監視單元；可區分為 P2P mode 與 Client mode。 P2P mode：其 WIFI 連線僅在手機與監視單元之間，無法連外，若手機有開啟行動通訊，則會基於安全性而要求關閉行動通訊功能。 Client mode：監視單元可經由 WIFI Router 等設備連至網際網路。 (1) 一般用戶： 僅具備查詢與瀏覽權限：    發電資訊    變流器資訊    歷史紀錄 「案場設定」頁面僅能瀏覽變流器資訊而無法進行變更，同 Remote Monitoring 的一般用戶。

圖示 2.2.6-1

(2) 進階用戶：進入現場設定（Local Setting）頁面，輸入授權之密碼後，可進行併網參數設定（Grid setting）及韌體更新（FW upgrade）



併網參數設定



韌體更新

2. 遠端監控（Remote Monitoring）：手機不連接監視單元，而是經由網際網路自雲端取得變流器相關資訊。

無進階用戶，只有一般用戶，僅具備查詢或瀏覽資訊之權限：

發電資訊

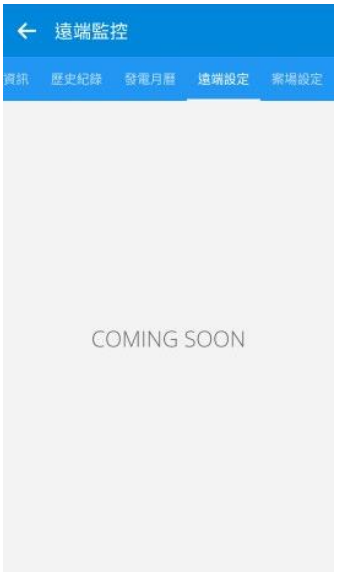
變流器資訊

圖示 2.2.6-1

歷史紀錄

發電月曆

雖有「遠端設定」頁面，但目前無內容可供設定；「案場設定」頁面無法變更資訊，「刪除」功能僅是將於變流器資訊自雲端移除，並未解除該變流器與帳號之綁定，在 DeltaSolar App 的本地監控（Local Monitoring）下仍可見到該變流器。



發電資訊

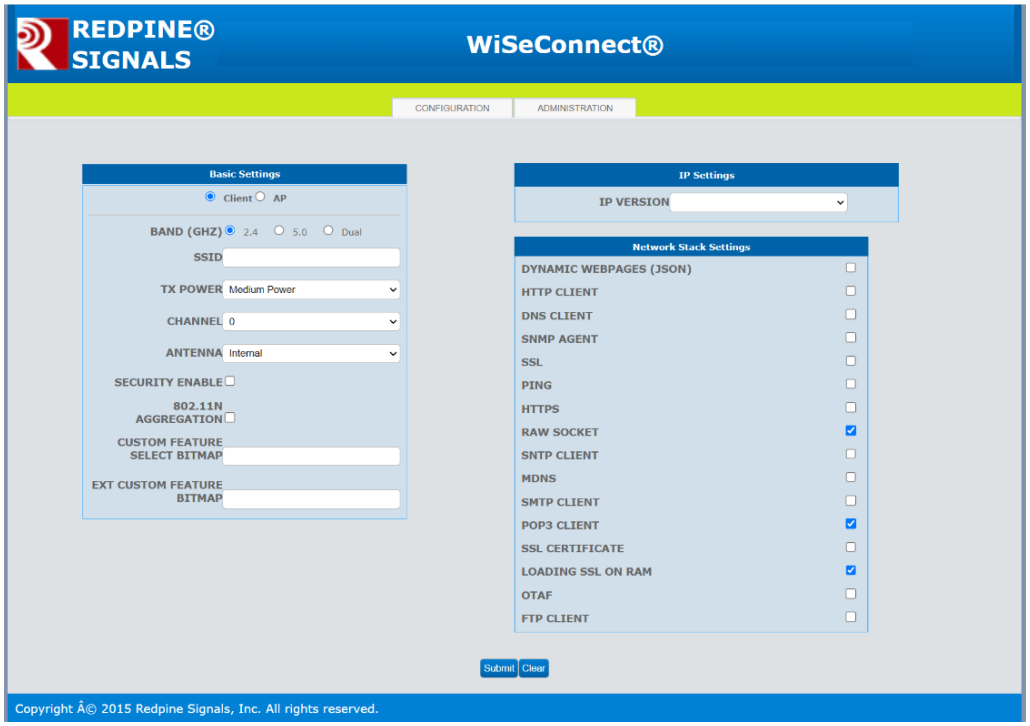
案場設定

刪除變流器

圖示 2.2.6-2

監視單元 WEB 介面

透過 WIFI 連接內嵌之監視單元，開啟瀏覽器並輸入：http://[PVI IP]即可存取此介面，此介面為 WIFI 晶片商（Redpine Signals）預設自帶的 WEB 管理介面，有兩個主要頁面：CONFIGURTAION 與 ADMINISTRATION。雖無身份鑑別之機制，然 port 80 僅在 P2P mode 下開啟，一旦進入 Client mode（可連上 internet）便關閉，此可由測項 2.3.1 得知；廠商亦於自檢表宣告其輔助措施（見附件一 測項 2.4.1 附加說明或佐證）。



CONFIGURTAION 頁面

ADMINISTRATION 頁面

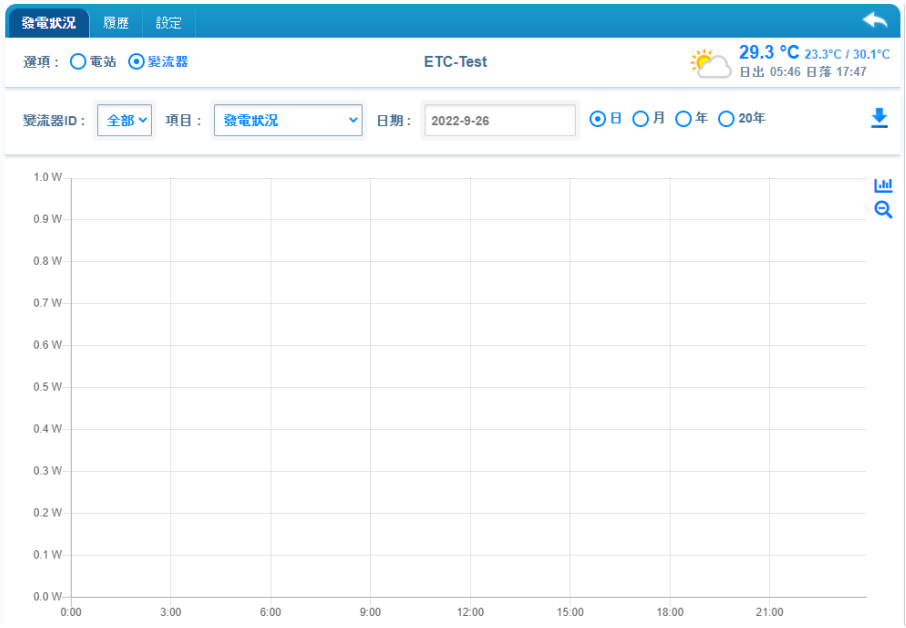
圖示 2.2.6-3

太陽能雲 WEB 介面

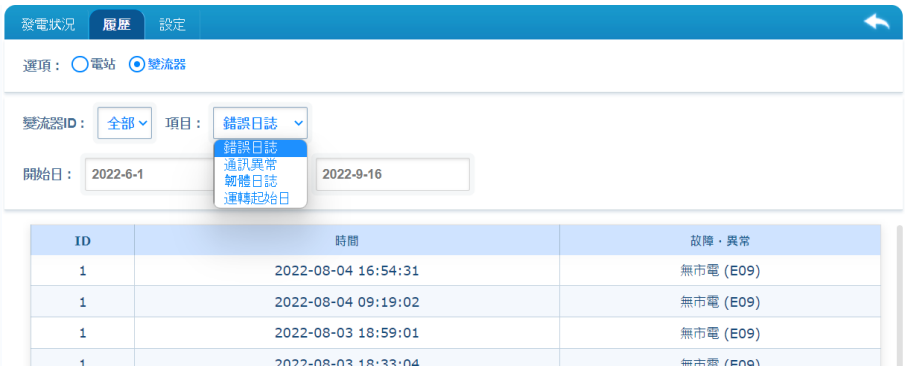
僅有一般用戶，除變更登入密碼外，僅可瀏覽發電或設備異常資訊。

1. 查詢或瀏覽資訊

   與手機之 Remote Monitoring 一般帳戶所看到的資訊大致相同，如：「發電狀況」、「履歷」（同於 DeltaSolar App 的「歷史紀錄」，即事件日誌）。



變流器發電狀況



變流器日誌

圖示 2.2.6-3

2. 變更密碼

3. 「設定」頁面僅可瀏覽，無法變更變流器資訊：

圖示 2.2.6-3

「刪除」功能同樣無法解除設備與帳號之綁定，只是將變流器資訊自雲端中移除。

2.2.7 事件日誌

A. 測試說明

監視單元應具備事件日誌功能，或經由管理系統之支援達成此項要求。

B. 測試方法

1. 事件日誌可存在於監視單元（本地端）或管理系統（遠端）內。
2. 事件日誌應至少包含：軟/韌體更新紀錄、緊急/異常事件及遠端遙控事件（如有遠端控制功能），且每一事件應可由紀錄中辨識事件時間、事件種類與誘發事件之來源身份（可能為人員或設備）。
3. 廠商應提供存取事件日誌之操作程序說明，並提供具權限之帳號。登入具權限之帳號並存取、瀏覽事件日誌，確認有符合步驟 2 之要求，否則判為不符合。
4. 登入較低權限之帳號，應無法刪除或修改事件日誌，否則判為不符合。

C. 預期結果

1. 事件日誌存在於監視單元（本地端）或管理系統（遠端）內。

2. 事件日誌至少包含：

(1) 軟/韌體更新紀錄
(2) 緊急/異常事件
(3) 遠端遙控事件（如有遠端控制功能）
且每一事件可由紀錄中辨識事件時間、事件種類與誘發事件之來源身份。

3. 依廠商所提供之帳號及操作程序登入後，存取、瀏覽事件日誌，其符合前項之要求。

4. 登入較低權限之帳號，無法刪除或修改事件日誌。

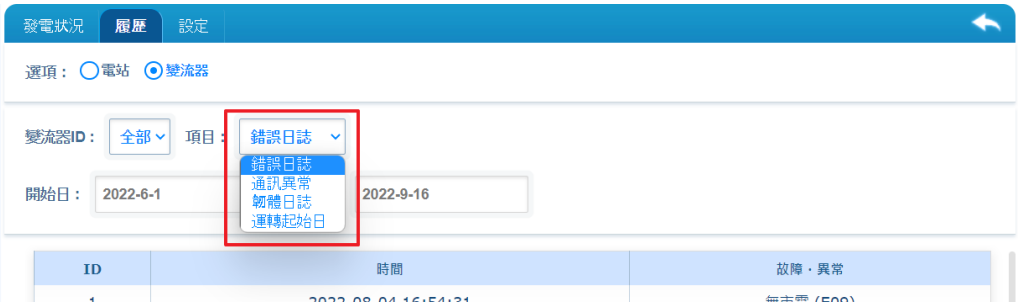
- 檢測結果

說明	結果
1. 事件日誌可於變流器（見測項 2.2.2）、DeltaSolar 及雲端（太陽能雲，見測項 2.2.6）中存取，其內容相同。 2. 事件日誌種類包含（圖示 2.2.7-1）： (1) 韌體日誌（韌體更新紀錄）：來源身份僅有進階用戶。 (2) 錯誤日誌（緊急/異常事件）：來源身份為設備 ID。 (3) 通訊異常（緊急/異常事件）：來源身份為設備 ID。 (4) 運轉起始日：目前測試樣機無紀錄。 (5) 其遠端遙控事件即韌體更新事件。 綜上所述，故判定為符合。	■符合 □不符合

- 檢測結果截圖說明

圖示 2.2.7-1

1. 日誌種類：



2. 韌體日誌（韌體更新紀錄）：

3. 錯誤日誌（緊急/異常事件）：

圖示 2.2.7-1

4. 通訊異常（緊急/異常事件）：

5. 運轉起始日：

2.2.8 事件日誌之儲存容量與效期

A. 測試說明

廠商應能預期監視單元或管理系統之事件日誌之儲存容量與效期。

B. 測試方法

1. 廠商應提供事件日誌保存方式與預期儲存時間之說明。
2. 廠商應說明對產品之事件日誌保存期限之需求及原因，且步驟 1 之預期儲存時間應高於此需求。
3. 廠商應說明事件日誌儲存量瀕臨或超過其儲存空間時之應對方式（如定期將事件日誌上傳管理系統，而不會一直累積於監視單元內），並確保不會造成監視單元故障。
4. 審閱上述說明文件，確認廠商均能提出合理說明，則本項

符合。

C. 預期結果

1. 對於事件日誌保存方式與預期儲存時間，廠商能提供合理之說明。
2. 對於產品之事件日誌保存期限之需求及原因，廠商能提供合理之說明，且前項之預期儲存時間高於此需求。
3. 對於事件日誌儲存量瀕臨或超過其儲存空間時，廠商能合理說明其應對方式，並確保不會造成監視單元故障。

- 檢測結果

說明	結果
依自檢表宣告： 1. 雲端的日誌保存方式為將資料儲存於資料庫管理系統。 2. 日誌定期備份（見圖示 2.2.8-1）。 3. 預期資料儲存時間為至少保存 20 年。 4. 若雲端儲存的事件日誌超過存放空間，則會進行硬碟儲存空間擴充，並有「雲端日誌管理 SOP」文件作為指引（見圖示 2.2.8-1）。 綜上所述，故判定為符合。	■符合 □不符合

- 檢測結果截圖說明

圖示 2.2.8-1
「雲端日誌管理 SOP」文件： 1. 日誌定期備份

圖示 2.2.8-1

每天進行備份(資料庫DUMP至異地伺服器)

每天會將資料庫備份檔案進行異地備份(離線server)

Name	Date modified	Type	Size
mysql-bin.002179	9/22/2022 12:22 PM	002179 File	618,132 KB
mysql-bin.002178	9/22/2022 8:26 AM	002178 File	1,048,577 ...
mysql-bin.index	9/22/2022 8:26 AM	INDEX File	64 KB
mysql-bin.002177	9/22/2022 1:46 AM	002177 File	1,048,577 ...
mysql-bin.002176	9/21/2022 7:01 PM	002176 File	1,048,594 ...
mysql-bin.002175	9/21/2022 12:21 PM	002175 File	1,048,577 ...
mysql-bin.002174	9/21/2022 5:42 AM	002174 File	1,048,577 ...
mysql-bin.002173	9/20/2022 10:52 PM	002173 File	1,048,577 ...
mysql-bin.002172	9/20/2022 4:11 PM	002172 File	1,048,577 ...
mysql-bin.002171	9/20/2022 9:37 AM	002171 File	1,048,577 ...
mysql-bin.002170	9/20/2022 2:48 AM	002170 File	1,048,577 ...

2. 偵測日誌剩餘空間

透過Server Manager管理工具來偵測Disk使用量，若超過90%則Percent used會顯示紅色警告。

VOLUMES
All volumes | 7 total

Filter

Volume	Status	File System Label	Provisioning	Capacity	Free Space	Deduplication Rate	Deduplication Savings	Percent Used
SGMSAZDSOLAR (7)								
\\?\Volume{ef5...		System Reserved	Fixed	350 MB	87.9 MB			
D:		Temporary Storage	Fixed	256 GB	256 GB			
G:		New Volume	Fixed	100 GB	77.6 GB			
C:			Fixed	512 GB	455 GB			
E:		Data Disk	Fixed	2.00 TB	1.19 TB			
H:		New Volume	Fixed	2.00 TB	605 GB			
F:		New Volume	Fixed	100 GB	77.9 GB			

Last refreshed on 9/22/2022 12:18:47 PM

3. 硬碟擴充流程

1. 發生硬碟容量不足
2. 提出IT Virtual Service Change Request表單 (如圖)
3. 主管逐層簽核
4. IT設定Azure VM 硬碟配置

VM Spec. Change

Hostname : Datacenter :
Env. : to
Start Date : to
CPU : to
RAM (GB) : to
1st Disk (GB) : 512 to
2nd Disk (GB) : 4000 to
IP : to
End Date : to
Primary Owner : to
Secondary Owner : to

保存 關閉

2.3 通訊資安

2.3.1 最小通訊埠要求

A. 測試說明

監視單元不應存在未知之網路埠。

B. 測試方法

1. 廠商應說明其產品開通之通訊埠與開通原因，啟用之通訊埠應符合最少權限原則。若存在非必要之通訊埠或未能提供說明者，本項為不符合。
2. 將產品與測試電腦連接，啟用具網路埠掃描功能之工具，對產品執行 TCP 埠、UDP 埠及埠 0 之掃描。
3. 比對掃描結果是否與廠商說明一致，若內容相符，則本項為符合。

C. 預期結果

1. 廠商能說明其產品開通之通訊埠與開通原因，啟用之通訊埠亦符合最少權限原則，不存在非必要之通訊埠。
2. 對產品執行 TCP 埠、UDP 埠及埠 0 之掃描後，其掃描結果與廠商說明一致。

- 檢測結果

說明	結果
1. 依自檢表宣告預設開啟的通訊埠及其服務： (1) TCP ● port 5001 for P2P Modbus TCP ● port 502 for P2P Modbus TCP ● port 443 for HTTPS（Client mode） ● port 80 for HTTP（P2P mode） (2) UDP：無開啟之通訊埠 2. 以 nmap 對監視單元進行 TCP 埠及埠 0 之掃描後，其開啟之	■符合 □不符合

通訊埠/服務與廠商宣告一致（見圖示 2.3.1-1） 3. 以 masscan 對監視單元進行 UDP 埠及埠 0 之掃描後，無開啟之通訊埠及其服務，與廠商宣告一致（見圖示 2.3.1-2）。 綜上所述，故判定符合。	

- 檢測結果截圖說明

圖示 2.3.1-1

P2P mode 下掃描 TCP port0 ~ port 65535 之結果：

```
┌──(root💀kali)-[/home/kali]
└─# nmap -n -p 0-65535 192.168.50.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-25 11:52 CST
Nmap scan report for 192.168.50.1
Host is up (0.014s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
502/tcp  open  mbap
5001/tcp open  commplex-link
MAC Address: 80:C9:55:12:55:A8 (Redpine Signals)

Nmap done: 1 IP address (1 host up) scanned in 55.82 seconds
```

Client mode 下掃描 TCP port0 ~ port 65535 之結果：

```
PS C:\Windows\system32> nmap -p 0-65535 192.168.137.133
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-04 13:22 台北標準時間
Nmap scan report for 192.168.137.133
Host is up (0.084s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE    SERVICE
443/tcp  open     https
502/tcp  filtered mbap
5001/tcp filtered commplex-link
MAC Address: 80:C9:55:12:55:A8 (Redpine Signals)
```

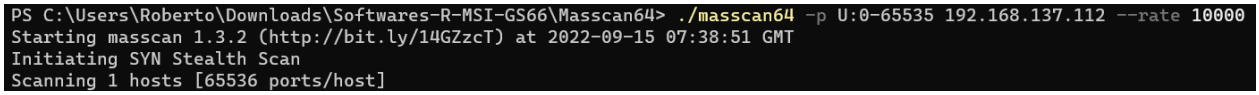
圖示 2.3.1-2

P2P mode 下掃描 UDP port0 ~ port 65535 之結果：

```
┌──(root💀kali)-[/home/kali]
└─# masscan 192.168.50.1 -p U:0-65535 --rate 10000
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-08-25 03:49:34 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [65536 ports/host]
```

圖示 2.3.1-2

Client mode 下掃描 UDP port0 ~ port 65535 之結果：



2.3.2 動態資料加密保護

A. 測試說明

應對透過監視單元傳輸之機敏資料進行加密保護。

B. 測試方法

1. 機敏資料之定義請參考測試項目 2.2.4。
2. 將監視單元連接至網際網路並與測試電腦處於同一網域，持續以測試電腦監聽/側錄往來監視單元之封包。
3. 側錄期間，依廠商之操作說明，登入帳戶並對監視單元進行存取動作。
4. 檢視側錄之封包，應無法查看到機敏資料未經加密之明文，否則本項次為不符合。

C. 預期結果

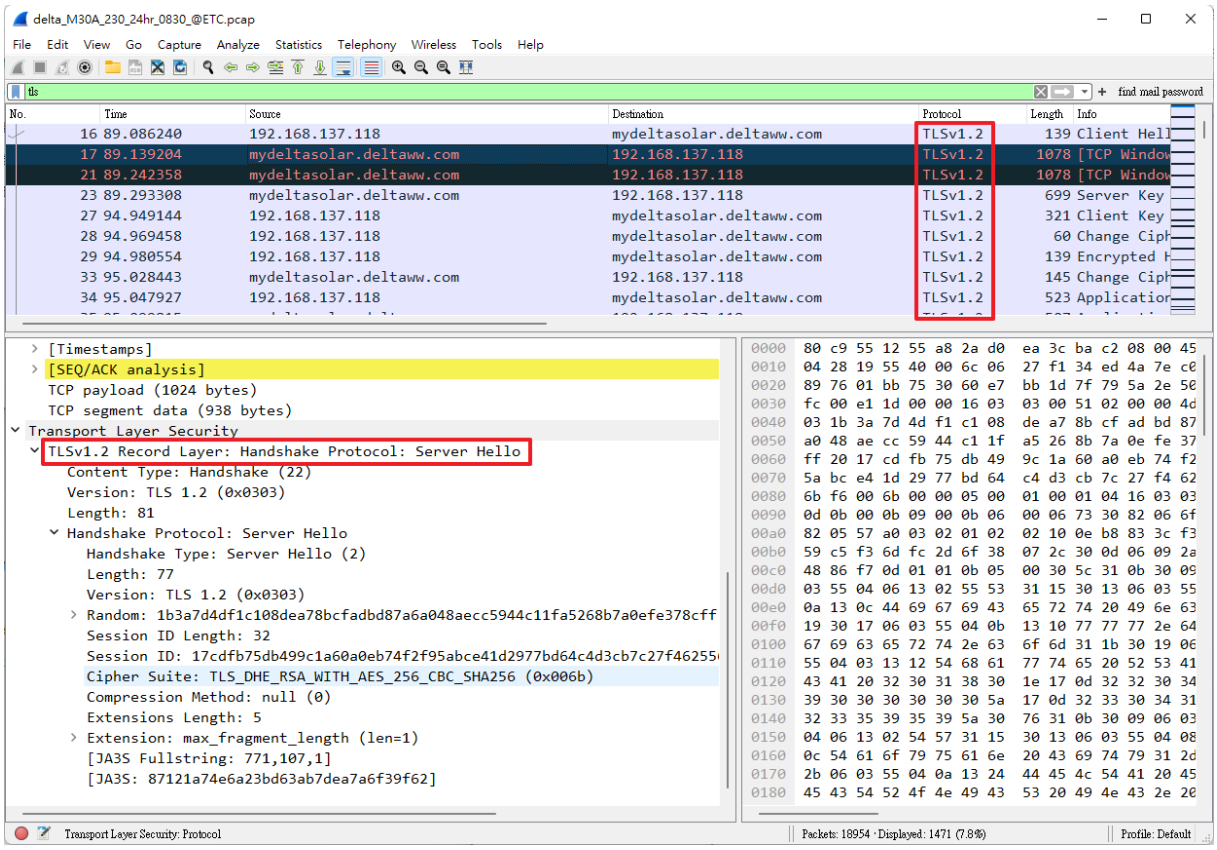
檢視側錄之封包，無法查看到機敏資料未經加密之明文。

- 檢測結果

說明	結果
依自檢表宣告：監視單元與主雲端伺服器連線資料均透過 HTTPS TLS1.2。 經檢測，其傳輸確實如廠商所述採 TLS 1.2 加密連線（見圖示 2.3.2-1），故判定為符合。	■符合 □不符合 □不適用

- 檢測結果截圖說明

圖示 2.3.2-1



2.3.3 動態資料加密保護—進階

A. 測試說明

監視單元與管理系統間之資料傳輸應採用符合 FIPS 140-2 要求之密碼模組進行資料保護。

B. 測試方法

1. 由廠商提供監視單元與管理系統間資料傳輸所採用加密方式之說明與佐證資料，其加解密用金鑰的保密機制應採用符合 FIPS 140-2 要求之密碼模組。
2. 審閱廠商提供之資料以確認符合本測試項目要求。

C. 預期結果

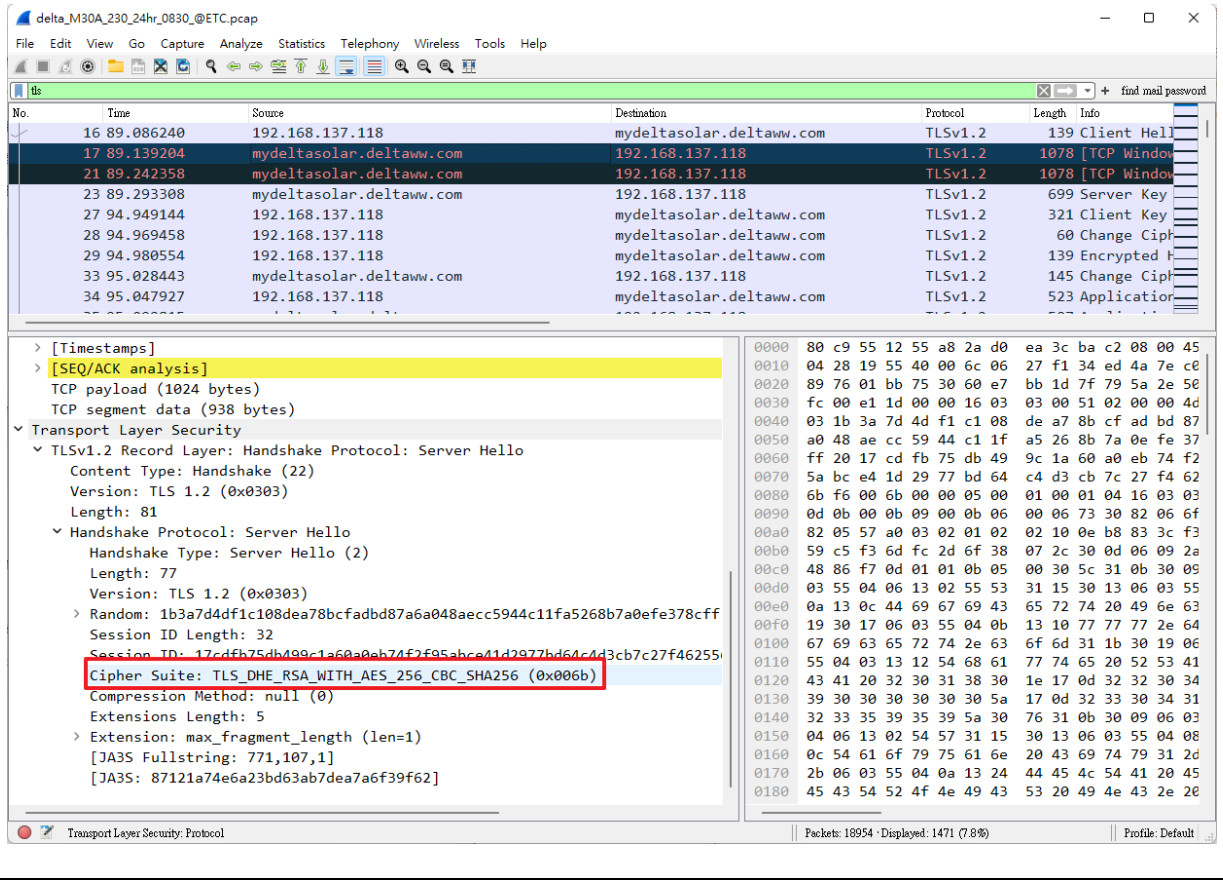
經測試並核對廠商所提供之說明與佐證資料後，其加解密用金鑰的保密機制確實採用符合 FIPS 140-2 要求之密碼模組。

- 檢測結果

說明	結果
承測項 2.3.2，檢視 TLS 1.2 封包之所採之密碼模組，符合 FIPS 140-2 之要求，故判定為符合。	■符合 □不符合

- 檢測結果截圖說明

圖示 2.3.3-1



2.3.4封包流量與指向分析

A. 測試說明

監視單元連接網路時不應對未宣告的 IP 進行封包傳遞。

B. 測試方法

1. 廠商應宣告監視單元預期會連結之伺服器 IP 位址及其他可能位置，並提供合理數據流量之說明資料。
2. 將監視單元連接至網際網路並與測試電腦處於同一網域，持續以測試電腦監聽/側錄往來監視單元之封包至少 24 小時。
3. 檢查側錄之封包，其目的地位址應與廠商自我宣告後台伺服器連線目的地之 IP/DNS 相符，否則本項不符合。
4. 檢視側錄之封包流量，如有發現異常流量而廠商無法說明，則此項不符合。

C. 預期結果

1. 檢查側錄之封包，其目的地位址與廠商自我宣告後台伺服器連線目的地之 IP/DNS 相符。
2. 檢視側錄之封包流量，未發現異常流量；如有，廠商能提出合理之說明。

- 檢測結果

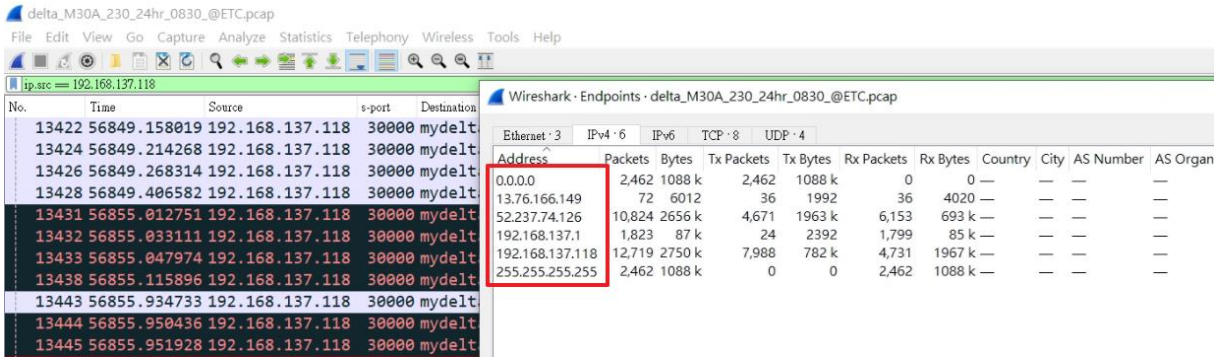
說明	結果
1. 廠商宣告封包流向之 IP 有： (1) 52.237.74.126 功能/原因：雲端伺服器 IP (2) 13.76.166.149 功能/原因：Microsoft Singapore 伺服器。 側錄封包並檢視其流向之 IP，其結果誠如廠商所宣告（見圖示 2.3.4-1），故判定為符合。	■符合 □不符合

- 檢測結果截圖說明

圖示 2.3.4-1

流向之 IP 如下圖紅框處：

排除 192.168.137.x（內網）、255.255.255.255（廣播）及 0.0.0.0（DHCP 客戶端還未獲取 IP 時，以此作「源地址」），其餘 IP（13.76.166.149、52.237.74.126）則與廠商宣告一致。



2.4 身份鑑別

2.4.1 人員使用者識別與鑑別

A. 測試說明

監視單元對人員使用者應予識別與鑑別。

B. 測試方法

1. 廠商應就測項 2.2.6 步驟 1 列出之所有人員使用者可存取產品之途徑，提供使用者識別與鑑別機制之說明。
2. 審閱廠商說明，並進行人員使用者登入，檢驗識別與鑑別機制是否符合廠商說明。

C. 預期結果

登入檢驗後，其識別與鑑別機制符合廠商之說明。

- 檢測結果

說明	結果
依自檢表所宣告： 1. 監視單元的 WEB 介面為 WIFI 晶片商（Redpine Signals）預設自帶的管理介面。 2. 此介面僅在 P2P mode 下開啟。 3. 此介面無帳號及身分鑑別機制。 4. 因無法由晶片商處取得源碼，故無法對此進行修改。 5. 廠商的輔助措施： (1) 變流器正常模式下為 Client mode，用來長時間監控發電資訊。 (2) P2P mode 須在工程人員在時才會使用，用來設定相關參數與更新韌體。 (3) 設定完後，會立即將 P2P mode 切換成 Client mode，80 port 會直接關閉 綜上所述，廠商對此介面有輔助措施，故判定為符合。	■符合 □不符合

2.4.2通行碼強度（長度基礎）

A. 測試說明

若採通行碼做為鑑別機制，則通行碼應有長度要求，以防止被暴力破解。

B. 測試方法

1. 依測項 2.2.6 與 2.4.1，除廠商特意申明之最低權限使用者，餘人員使用者若以通行碼做為鑑別機制，則其通行碼應有長度要求。
2. 若通行碼為人員使用者自行定義，則不應限定通行碼為固定長度(如限定僅能輸入 4 碼)，否則本項不符合。

3. 若採用預設通行碼而未強制使用者更新，則此預設通行碼不得為：
   (1) 可公開可取得之資訊(如登載於產品說明書內)。
   (2) 公認之弱通行碼形式，如：與帳號相同、採常見預設通行碼或單詞(ex. admin, root, password)、 重複字元(ex. kkkkk)、低於 8 碼之純數字組合、鍵盤按鍵順序組合(ex. qwerty)等。
4. 檢視廠商說明並進行相應帳號登入操作，驗證通行碼要求與廠商說明相符，則本項符合。

C. 預期結果

1. 若監視單元以通行碼做為鑑別機制，除最低權限使用者外，其餘人員使用者有其通行碼之長度要求。
2. 若通行碼為人員使用者自行定義，則通行碼不限定為固定長度。
3. 若採預設之通行碼作為鑑別符，則有強制使用者更新通行碼之機制；若否，則預設通行碼非為(1)可公開取得之資訊，或(2)公認之弱通行碼形式。
4. 依廠商說明並進行相應帳號登入操作，其通行碼要求與廠商說明相符。

- 檢測結果

說明	結果
依測項 2.4.1 所述，該介面無身份鑑別機制，無通行碼之採用，故本測項不適用。	□符合 □不符合 ■不適用

2.4.3 通行碼輸入頻次限制

A. 測試說明

採通行碼做為鑑別機制，應有通行碼輸入次數之限制，以防止被暴力破解。

B. 測試方法

1. 依測項 2.2.6 與 2.4.1，除廠商特意申明之最低權限使用者，餘人員使用者若以通行碼做為鑑別機制，則其通行碼輸入錯誤容許次數應為 5 次(含)以下，超過容許之登入次數時，介面應有重置或時間間隔鎖定機制。若非採通行碼為鑑別機制，則本項可申明為不適用。
2. 依廠商提供之測試帳號及通行碼登入產品，應能成功登入。後以錯誤之通行碼再登入，應登入失敗，且超過通行碼輸入錯誤容許次數後，應有重置或時間間隔鎖定機制，否則此測項不符合。

C. 預期結果

1. 若監視單元以通行碼做為鑑別機制，除最低權限使用者外，餘人員使用者其通行碼輸入錯誤容許次數為 5 次(含)以下；超過容許之登入次數時，則介面將啟動重置或時間間隔鎖定機制。
2. 依廠商提供之測試帳號及通行碼登入產品，可成功登入。後以錯誤之通行碼再登入，則登入失敗，且超過通行碼輸入錯誤容許次數後，將啟動重置或時間間隔鎖定機制。

- 檢測結果

說明	結果
依測項 2.4.1 所述，該介面無身份鑑別機制，無通行碼之採用，故本測項不適用。	□符合 □不符合 ■不適用

2.4.4 預設通行碼變更機制

A. 測試說明

人員使用者之初次鑑別若採公開取得之預設通行碼，則使用者首次登入後，應有要求預設通行碼變更之機制。

B. 測試方法

1. 依測項 2.2.6 與 2.4.1，除廠商特意申明之最低權限使用者，

餘人員使用者若採可公開取得之帳號或通行碼(如標示於產品說明書內)，應有強制使用者更新之機制。若無可公開取得之帳號或通行碼，本項可申明為不適用。

2. 依可公開取得之帳號及/或通行碼登入產品，應能成功登入。

3. 首次登入成功後，組件或系統應要求更改預設通行碼，且對通行碼之要求符合通行碼長度要求，否則本項不符合。

C. 預期結果

1. 除最低權限使用者，餘人員使用者若採可公開取得之帳號或通行碼，則有強制使用者更新之機制。

2. 依可公開取得之帳號及/或通行碼登入產品，能成功登入。

3. 首次登入成功後，組件或系統會要求更改預設通行碼，且通行碼符合長度要求。

- 檢測結果

說明	結果
依測項 2.4.1 所述，該介面無身份鑑別機制，無可公開取得之帳號或通行碼，故本測項不適用。	□符合 □不符合 ■不適用

附件一 廠商自我檢查表

變流器本體單元廠商自我檢查表

基本資訊			
申請者	台達電子工業股份有限公司台南分公司	填表日期	2022/09/14
樣品名稱	太陽能變流器	型號	主：M30A_230 系列：M30A_231 / M20A_220
變流器是否具備內嵌式監視單元？		■是 請額外填寫監視單元廠商自我檢查表 □否 (請提供佐證資料)	

產品名稱	資安要求	資安等級	自我檢查	附加說明或佐證
變流器本體單元	1.1.1 實體防護	2	■符合 □不符合	本系列產品採用一次性貼紙作為實體防護之措施
	1.2.1 軟/韌體更新機制	1	■符合 □不符合	本系列**各機種**之韌體更新方式與保護機制皆相同。 本系列**各韌體**之更新方式與保護機制皆相同。 1. 可更新之韌體版本： **COMM.：V1.20** M30_15A2X0_COMM_V0120_D2209.HEX Hash CRC32: b8d0414b **DSP1：V1.16** M30_15A2X0_DSP1_V0116_D2209_DBV7.HEX Hash CRC32: 27dc3641 **DSP2：V1.02** M30A230_DSP2_V0102_D2037_DBV7.HEX Hash CRC32: 2dd0d26b **RED：V1.03** M30A_230_RED_V0103_D2048_B5.HEX Hash CRC32: ff158205 2. 軟/韌體更新保護機制說明文件 (1) 更新後不會造成產品的系統時間、事件日誌被重置為預設狀態。本產品未設置登入帳號，故無登入帳號重置的問題；測項 1.3.2 中，無線介面之身分鑑別，其帳號與通行碼是由手機 app 來進行鑑別，而非由變流器。 (2) 遭竄改及錯誤韌體拒絕之機制，是由被授權更新之人員（包含工程人員或經銷商的安裝人員）比

1

				對韌體 hash 值來實現，以避免竄誤之韌體燒錄至變流器。 詳細比對步驟請參考： →韌體更新前比對 hash 值的 SOP 說明.pdf 3. 更新軟/韌體之操作程序 產品出廠後，並不預期會頻繁之韌體更新需求，如需更新，需透過 RS485 排線連接電腦與變流器與 RS485 孔連接，電腦內需安裝專用之韌體燒錄程式（Delta_Solar_System (DSS).exe）以進行更新，此外，可由手機 DeltaSolar app 進階權限進行更新，然僅更新介面不同，保護機制皆與前者一致。 詳細更新步驟請參考：韌體燒錄程式說明.pdf 4. 可供更新之檔案 檢測前提供即可（除新舊韌體檔外，若須透過軟體進行更新，也請提供該軟體名稱） (1)韌體檔： A. 更新用韌體檔及其對應版本號： **COMM.：V1.20** M30_15A2X0_COMM_V0120_D2209.HEX Hash CRC32: b8d0414b **DSP1：V1.16** M30_15A2X0_DSP1_V0116_D2209_DBV7.HEX Hash CRC32: 27dc3641 **DSP2：V1.02** M30A230_DSP2_V0102_D2037_DBV7.HEX Hash CRC32: 2dd0d26b **RED：V1.03** M30A_230_RED_V0103_D2048_B5.HEX Hash CRC32: ff158205 B. 更新前韌體檔及其對應版本號： **COMM.：V1.19** M30A230_EU_COMM_V0119_D2152.HEX Hash CRC32: 9e6c2295 **DSP1：V1.15** M30_15A2X0_DSP1_V0115_D2152_DBV7.HEX Hash CRC32: f56ee5f2 **DSP2：V1.01** M30A230_DSP2_V0101_D1949_ DBV7.HEX Hash CRC32: 49206299

2

				RED：V1.02 M30A_230_RED_V0102_D2036_B5.HEX Hash CRC32: 96ccec45 (2)軟體檔： Delta_Solar_System (DSS).exe 5. 具更新權限之帳戶 (1) 本系列機種僅支援本地端更新（使用 Delta 燒錄 tool(DSS)透過有線 485 做更新） (2) 燒錄軟體 DSS 可由公司官網下載，但韌體 Hex 檔必須由授權工程人員提供，未公開予一般用戶下載；實際執行更新僅有本公司的工程人員或經銷商的安裝人員可為之。
	1.2.2 軟/韌體安全性評估	2	□符合 □不符合	將提供源碼進行檢測
	1.3.1 人機介面身分鑑別(實體)	1	□符合 □不符合 ■不適用	本系列產品之實體人機介面僅有燈號
	1.3.2 人機介面身分鑑別(無線)	1	■符合 □不符合 □不適用	1. 本系列產品具備 WI-FI 及 SUB_1G（選配）無線通訊功能。SUB_1G 須選配本司專屬之天線，並經由本司專屬之 Data Collector（監視單元），方可實現無線通訊之功能。 2. 因 SUB_1G 的無線人機介面設計於 APP（DeltaSolar）上，因此對於變流器本體而言，本測項不適用。 3. 操作說明：請參考「APP 操作說明 SUB 1G 藍芽.pdf(內含 Sub1G 的 APP 與 Bluetooth 的 APP 說明)」。 4. WIFI 無線人機介面則請參考監視單元之相關測項。

監視單元廠商自我檢查表.

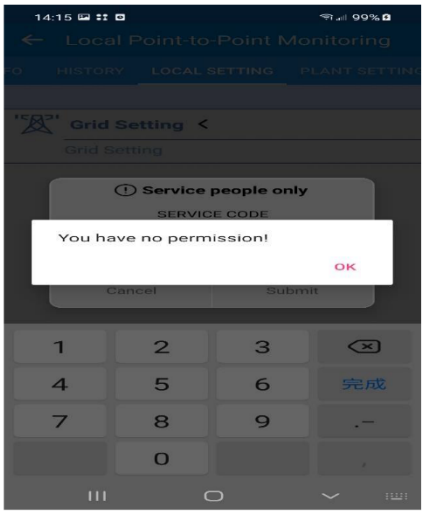
監視單元	
樣品樣態：	☐ Smart Dongle ☐ Data logger/ PV Gateway/Data Recorder ☐ 工業電腦+軟體程式 ■ 其他
監視單元是否可控制、修訂變流器本體單元之電力相關參數或遠端執行本體單元之軟/韌體更新？	■是 ☐否 雲端進階用戶可設定併網參數，如 2.2.6 項之說明。

產品名稱	資安要求	資安等級	自我檢查	附加說明或佐證
監視單元	2.1.1 實體防護	2	☐符合 ☐不符合	本系列產品採用星形螺絲搭配一次性貼紙作為實體防護之措施
	2.1.2 最小實體介面要求	1	■符合 ☐不符合	設備僅有 Wifi 天線，餘無外露之實體介面
	2.2.1 已知脆弱性掃描	1	☐符合 ☐不符合	可提供產品進行檢測
	2.2.2 軟/韌體更新機制	1	■符合 ☐不符合	1. 可更新之韌體： 更新用之版本：V1.03 PPM_N2_WiFi_COMM_V0103_D2216.HEX Hash CRC32: 1da384b2 更新前之版本：V1.02 PPM_N2_WiFi_COMM_V0102_D2134.HEX Hash CRC32: a6be42a9 2. 保護機制： (1) 產品的系統時間、事件日誌設置於變流器本體（參考測項 1.2.1），監視單元不具備該功能，故無更新後重置的問題。 (2) 遭竄改及錯誤韌體拒絕之機制，是由被授權更新之人員（包含工程人員或經銷商的安裝人員）比對韌體 hash 值來實現，以避免竄誤之韌體燒錄至變流器。 詳細比對步驟請參考： →韌體更新前比對 hash 值的 SOP 說明.pdf 3. 更新方式說明：

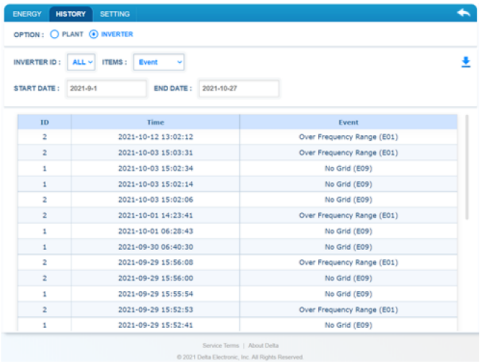
				產品出廠後，並不預期會頻繁韌體更新需求，如需更新，則於 P2P mode 下透過 WIFI 連接變流器並以燒錄軟體（DSS）進行韌體更新（請參考「韌體燒錄程式說明.pdf」），此外，可由手機 DeltaSolar app 進階權限進行更新，然僅更新介面不同，保護機制皆與前者一致。 4. 可供更新之檔案 (1) 測試用燒錄檔： A. 更新用體檔名稱及其對應版本： 更新用之版本：V1.03 PPM_N2_WiFi_COMM_V0103_D2216.HEX Hash CRC32: 1da384b2 B. 更新前之韌體檔名稱及其對應版本： 更新前之版本：V1.02 PPM_N2_WiFi_COMM_V0102_D2134.HEX Hash CRC32:a6be42a9 (2) 測試用軟體： Delta_Solar_System (DSS).exe DeltaSolar app 5. 具更新權限之帳戶 燒錄軟體 DSS 可由公司官網下載，但韌體 Hex 檔必須由授權工程人員提供，未公開予一般用戶下載；實際執行更新僅有本公司的工程人員或經銷商的安裝人員可為之。
	2.2.3 軟/韌體安全性評估	1	□符合 □不符合	將提供源碼後檢測方實施韌體掃描評估。
	2.2.4 機敏資料保護	1	□符合 □不符合 ■不適用	本系列機種皆無儲存機敏資料，故本測項不適用。
	2.2.5 惡意程式防護	2	□符合 □不符合	本監視單元為嵌入式系統，無獨立作業系統在內。
	2.2.6 帳戶管理	1	■符合 □不符合	1. App (1) Local Monitoring - P2P mode 及 Client mode A. 一般用戶：僅能查看發電或設備異常資訊。 帳號：sheng.lin@deltaww.com 密碼：Delta99999999

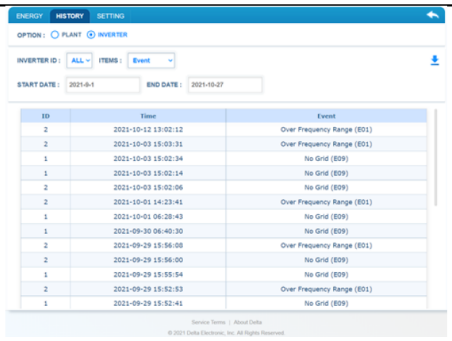
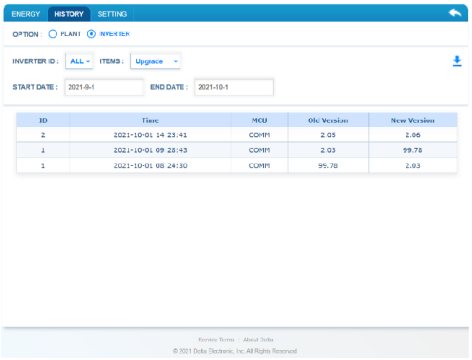
B. 進階用戶：可透過經授權之密碼做併網參數設定（Grid settings）及韌體更新（FW upgrade）

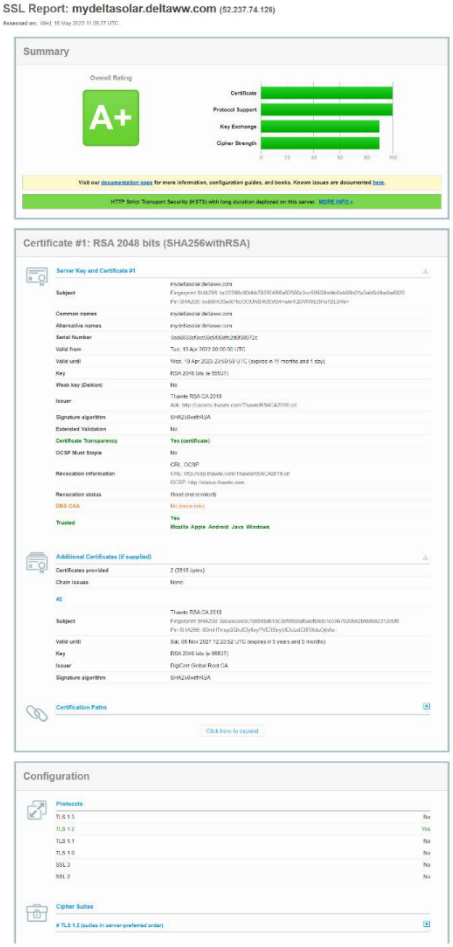
此為二階鑑別機制，須先通過一般用戶身分鑑別後，再輸入進階密碼變更為進階用戶，方可進入設定頁面。



(2) Remote Monitoring

				A. 一般用戶：權限同 Local Monitoring 之一般用戶。 B. 進階用戶：無。 2. 監視單元 WEB 介面：僅 P2P mode 下顯示 網址：http://[PVI IP] 此為 WIFI 晶片商（Redpine Signals）預設自帶的 WEB 管理介面；此介面無帳號及身分鑑別機制，然僅在 PSP mode 下可透過預設 80 port 進入，一旦進入 Client mode（可連上 internet）便關閉。  3. 雲端 WEB 介面 一般用戶：除變更其帳戶之登入密碼外，僅可瀏覽發電或設備異常資訊，為最低權限使用者。 網址：https://mydeltasolar.deltaww.com/ 帳號：sheng.lin@deltaww.com 密碼：Delta99999999 
	2.2.7 事件日誌	1	■符合 □不符合	1. 緊急/異常事件日誌： 分為 Fault、Error 和 Warning，由 Inverter 將事件上傳至雲端，雲端網頁會顯示事件以及發送信件通知用戶；手機亦可透過 DeltaSolar App 查看。

				 2. 韌體更新紀錄： 由雲端事件日誌可呈現該設備的韌體更新紀錄，包含更新日期和版本號。  3. 遠端控制事件 遠端控制事件即韌體更新。 以上日誌每一事件可由紀錄中辨識事件時間、事件種類與誘發事件之來源身分（可能為人員或設備）。 4. 存取管控： 裝置端上傳事件日誌至雲端後，資料無法刪除和修改。
	2.2.8 事件日誌之儲存容量/效期	2	□符合 □不符合	1. 雲端的日誌保存方式為將資料儲存於資料庫管理系統，並進行定期備份避免資料遺失。預期資料儲存時間為至少保存 20 年。 2. 若雲端儲存的事件日誌超過存放空間，則會進行硬碟儲存空間擴充。 請參考：雲端日誌管理 SOP.PPTX。
	2.3.1 最小通訊埠要求	1	■符合 □不符合	TCP port 5001 for P2P Modbus TCP TCP port 502 for P2P Modbus TCP TCP port 443 for HTTPS （Client mode） TCP port 80 for HTTP（P2P mode）

				UDP: 無
	2.3.2 動態資料加密保護	1	■符合 □不符合 □不適用	與主雲端伺服器連線資料均透過 HTTPS TLS1.2
	2.3.3 動態資料加密保護-進階	2	■符合 □不符合	資料傳輸為採用 TLS1.2，並參考佐證資料如下。 
	2.3.4 封包流量與指向分析	1	■符合 □不符合	側錄封包 24 小時。確認 IP 源、及傳輸量之合理性。 52.237.74.126 功能/原因：雲端伺服器 IP 13.76.166.149 功能/原因：Microsoft Singapore 伺服器。因採用 Microsoft Azure 虛擬機器，故選擇 Southeast Asia 資料中心(Singapore)提供服務，且與該伺服器間並未傳輸機敏資料。

	2.4.1 人員使用者識別與鑑別	1	■符合 □不符合	如測項 2.2.6 所述，本系列之變流器僅在 P2P mode 下開啟 80 port，可直接進入 WIFI 晶片商（Redpine Signals）預設自帶的 WEB 管理介面；此介面無帳號及身分鑑別機制，然因無法由晶片商處取得源碼，故無法對此進行修改。 而本司的輔助措施為： 1. 變流器正常模式下為 Client mode，用來長時間監控發電資訊 2. P2P 模式須在工程人員在時才會使用，用來設定相關參數與韌體更新 3. 設定完成後，會立即將 P2P mode 切換成 Client mode，80 port 會直接關閉
	2.4.2 密碼強度(長度基礎)	1	■符合 □不符合 □不適用	請參考測項 2.4.1 所述
	2.4.3 密碼輸入頻次限制	1	■符合 □不符合 □不適用	請參考測項 2.4.1 所述
	2.4.4 預設密碼變更機制	1	■符合 □不符合 □不適用	請參考測項 2.4.1 所述
*佐證資料：				
（若說明欄格位不足時，可以附註方式將必要資訊呈現於此欄位，本欄位不限格式、可自行延伸。）				

公司大小章用印處：

台達電子工業股份有限公司
台 南 分 公 司
商品驗證登錄專用章
海 英 俊

中華民國 111 年 9 月 14 日

附件二 系列差異表

變流器主型式及系列型式機種審定切結書

本公司__台達電子工業股份有限公司台南分公司__確認下列之記載完全符合事實，若因下列之記載不實而衍生之一切糾紛，願由本公司自行承擔。

(一)切結事由：以系列方式申請符合太陽光電變流器及監視單元資安檢測技術規範與商品驗證登錄認可。

(二)申請機種型號： **M30A_230、M30A_231、M20A_220**

(三)機種差異描述：(如不符使用可由廠商自行增修)

機種名稱 / 評估項目	主測型號 M30A_230	系列型號 M30A_231	系列型號 M20A_220
滿載 MPPT 電壓範圍	480~900V	○	480~900V
PV String 數量	6	× 6 (8) (參考附件說明)	× 4
額定輸出功率	30000W	○	20000W
額定輸出電壓	220Vac / 230Vac	○	○
額定輸出頻率	50Hz / 60Hz	○	○
最大輸出電流	50A	○	32A
輸出形式	三相併網型	○	○
韌體版本(1)	M30_15A2X0_COMM_V0120_D2209.HEX	○	○
韌體 HASH 值(1)	CRC32: b8d0414b	○	○
韌體版本(2)	M30_15A2X0_DSP1_V0116_D2209_DBV7.HEX	○	○
韌體 HASH 值(2)	CRC32: 27dc3641	○	○
韌體版本(3)	PPM_N2_WiFi_COMM_V0103_D2216.HEX	○	○
韌體 HASH 值(3)	CRC32:1da384b2	○	○

韌體版本(4)	M30A230_DSP2_V0102_D2037_DBV7.HEX	○	○
韌體 HASH 值(4)	CRC32:2dd0d26b	○	○
韌體版本(5)	M30A_230_RED_V0103_D2048_B5.HEX	○	○
韌體 HASH 值(5)	CRC32:ff158205	○	○
通訊介面	RS485 / WI-FI SUB-1G（選配）	○	○
其他說明	主型式與系列型式韌體更新方式一致 於資安測試之同系列認定可為： (1)操作介面相同且支援相同功能或支援較少功能之機型； (2)部份外觀形式、外部連線方式、部分韌體/軟體程式碼之參數設定值等，雖有差異，然不影響資安檢測判定或僅少數項目需增加測試之機型。 (3)PV String 數量，請參考圖示說明。		
註：(1)完全一致請標示〝○〞。 (2)未完全一致請標示〝x〞，並說明差異處。			

(四)除上列事實外，本公司提請中華民國經濟部標準檢驗局變流器資訊安全型式認可之文件資料，僅提供差異部份之機種及說明，其未附部份表示所有機種完全一致，特此說明。

立切結書人(公司名稱)：台達電子工業股份有限公司台南分公司

公司大小章：

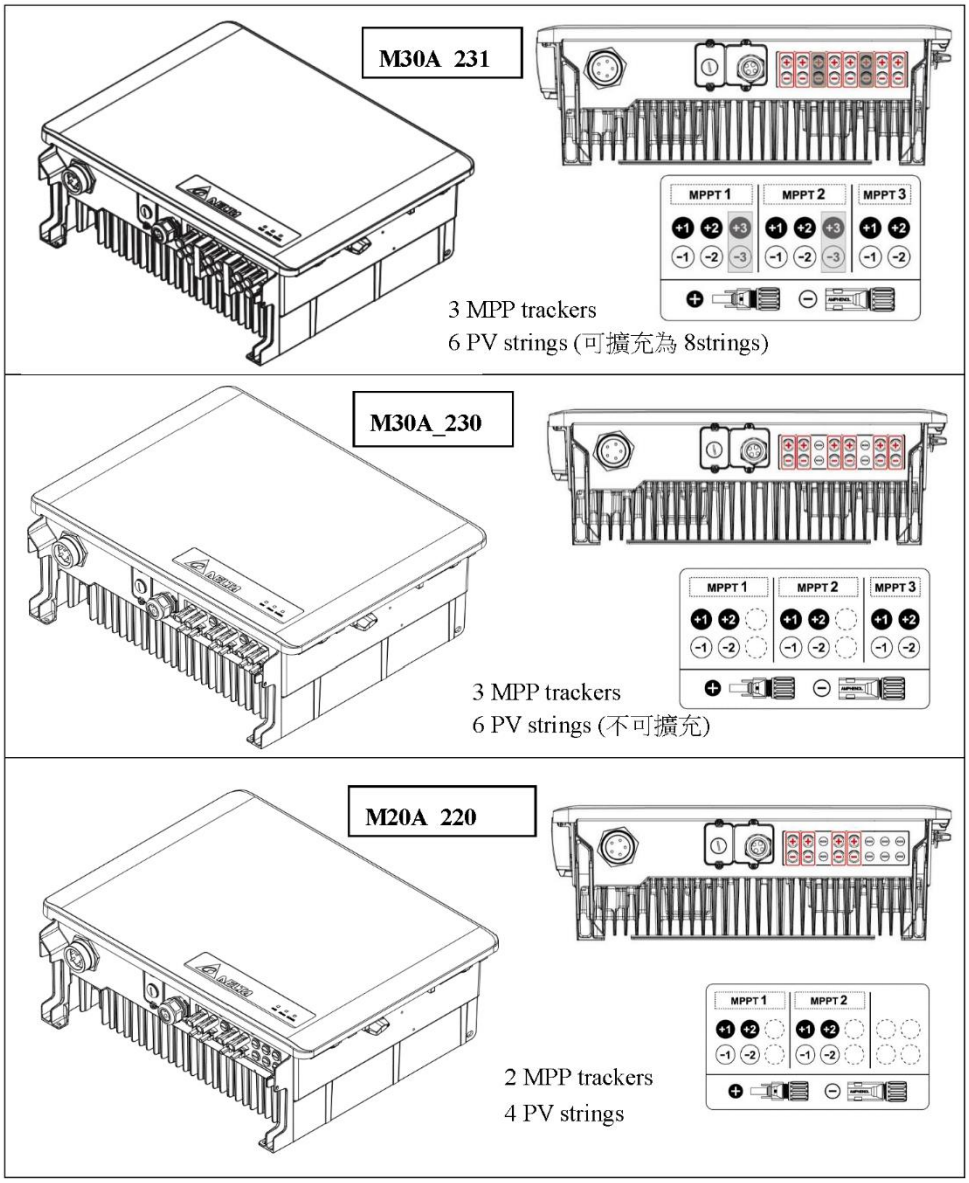
台達電子工業股份有限公司
台 南 分 公 司
商品驗證登錄專用章
海 英 俊

地址：台南市善化區 7 鄰環東路二段 39 號 聯絡人：張崇逸/邱子鵬

負責人：海英俊 TEL：06-505-6565 FAX：06-505-1919

中華民國 111 年 9 月 14 日

PV String 數量：


M30A 231
MPPT 1
MPPT 2
MPPT 3
3 MPP trackers
6 PV strings (可擴充為 8strings)
M30A_230
MPPT 1
MPPT 2
MPPT 3
3 MPP trackers
6 PV strings (不可擴充)
M20A 220
MPPT 1
MPPT 2
2 MPP trackers
4 PV strings

附件三 送測產品摘要表

送測產品摘要表（本體單元）

基本資訊：

商品名稱	變流器(內嵌監視單元)（太陽能變流器）
申請人	台達電子工業股份有限公司台南分公司
生產廠場	中達電子(江蘇)有限公司 台達電子工業股份有限公司平鎮廠
廠牌	台達電子

若為系列則請填寫下表：

		型式	規格	測試樣機序號	韌體版本號
主型式	本體單元	M30A_230	AC :400 V/ 380 V / 50/60HZ / 30kW	OAZ21800001W0	**通訊：V1.20** M30_15A2X0_COMM_V0120_D2209.HEX Hash CRC32: b8d0414b **DSP1：V1.16** M30_15A2X0_DSP1_V0116_D2209_DBV7.HEX Hash CRC32: 27dc3641 **DSP2：V1.02** M30A230_DSP2_V0102_D2037_DBV7.HEX Hash CRC32: 2dd0d26b **RED：V1.03** M30A_230_RED_V0103_D2048_B5.HEX Hash CRC32: ff158205 **WI-FI：V1.03**
	監視單元	RS9113-N00-S1C（WIFI）	DC 3.3V	OAZ21800001W0	
系列型式	本體單元	M30A_231	AC :400 V/ 380 V / 50/60HZ / 30kW	OAZ21800539W0	
	監視單元	RS9113-N00-S1C（WIFI）	DC 3.3V	OAZ21800539W0	
系列型式	本體單元	M20A_220	AC :400 V/ 380 V / 50/60HZ / 20kW	OCE21700249W0	
	監視單元	RS9113-N00-S1C（WIFI）	DC 3.3V	OCE21700249W0	

					PPM_N2_WiFi_COMM_ V0103_D2216.HEX Hash CRC32: 1da384b2
備註：韌體版本的 Master / Slave / Display 欄位僅為示例，若不相符，可依送測產品實際之韌體分類名稱逕行修改。					

公司大小章用印處：

台達電子工業股份有限公司
台 南 分 公 司
商品驗證登錄專用章
海 英 俊

中華民國 111 年 9 月 13 日

附件四 送測產品外觀圖及其內部俯視圖

主型式		**M30A_230**
	外觀圖	
	內部俯視圖	


Model / 型號 M30A_230
Solar Inverter / 太陽能變流器
P/N: RPI303M230100
DELTA
DC Input / 直流輸入
Max. Input Voltage / 最大輸入電壓 1000 Vd.c.
MPP Voltage Range / MPP電壓範圍 480 ~ 900 Vd.c.
Max. Input Current / 最大輸入電流 72 Ad.c.
Max. Short Circuit Current / 最大短路電流 50 Ad.c. per MPPT
AC Output / 交流輸出
Nominal Output Voltage / 額定工作電壓 400 / 380 Va.c.
Nominal Output Frequency / 額定工作頻率 50 / 60 Hz
Connection Type / 連接形式 3Ø3W / 3Ø4W, PE
Max. Continuous Output Current / 最大輸出電流 50 Aa.c.
Rated Continuous Output Power / 額定輸出功率 30000 W
Rated Apparent Output Power / 額定視在功率 30000 VA
Max. Apparent Output Power / 最大視在功率 33000 VA*
Power Factor / 功率因數 0.8 lead ~ 0.8 lag
*30000 VA max for AU/NZ
Protection Class / 保護等級 I
Over Voltage Category / 過電壓類別 III (AC), II (DC)
Ingress Protection / 防護等級 IP66
Operating Temperature Range / 操作溫度範圍 -25 ~ +60℃
Non-isolated inverter 非隔離型變流器
Manufacturing location: Made in China
No. 1688 Jiangxing East Road, Wujiang Economic Development Zone, Suzhou City, 215200 Jiangsu Province,P.R. China
Authorized representative
Delta Electronics (Netherlands) B.V.
Zandsteen 15, 2132 MZ Hoofddorp, The Netherlands
AS 4777.2:2020
IEC 61439-2
VPC
E-S,EMC
V63595-BSMI
60 sec.

系列型式	M30A_231	
	外觀圖	
	內部俯視圖	


Model / 型號 M30A_231
Solar Inverter / 太陽能變流器
P/N: RPI303M231100
DELTA
DC Input / 直流輸入
Max. Input Voltage / 最大輸入電壓 1000 Vd.c.
MPP Voltage Range / MPP電壓範圍 480 ~ 900 Vd.c.
Max. Input Current / 最大輸入電流 72 Ad.c.
Max. Short Circuit Current / 最大短路電流 50 Ad.c. per MPPT
AC Output / 交流輸出
Nominal Output Voltage / 額定工作電壓 400 / 380 Va.c.
Nominal Output Frequency / 額定工作頻率 50 / 60 Hz
Connection Type / 連接形式 3Ø3W / 3Ø4W, PE
Max. Continuous Output Current / 最大輸出電流 50 Aa.c.
Rated Continuous Output Power / 額定輸出功率 30000 W
Rated Apparent Output Power / 額定視在功率 30000 VA
Max. Apparent Output Power / 最大視在功率 33000 VA*
Power Factor / 功率因數 0.8 lead ~ 0.8 lag
*30000 VA max for AU/NZ
Protection Class / 保護等級 I
Over Voltage Category / 過電壓類別 III (AC), II (DC)
Ingress Protection / 防護等級 IP66
Operating Temperature Range / 操作溫度範圍 -25 ~ +60℃
Non-isolated inverter 非隔離型變流器
Manufacturing location: Made in China
No. 1688 Jiangxing East Road, Wujiang Economic Development Zone, Suzhou City, 215200 Jiangsu Province,P.R. China
Authorized representative
Delta Electronics (Netherlands) B.V.
Zandsteen 15, 2132 MZ Hoofddorp, The Netherlands
AS 4777.2:2020
IEC 61439-2
E-S,EMC V63595-BSMI
60 sec.

系列型式		**M20A_220**
	外觀圖	
	內部上視圖	


Model / 型號 M20A_220
Solar Inverter / 太陽能變流器
P/N: RPI203M220100
DELTA
DC Input / 直流輸入
Max. Input Voltage / 最大輸入電壓 1000 Vd.c.
MPP Voltage Range / MPP電壓範圍 480 ~ 900 Vd.c.
Max. Input Current / 最大輸入電流 48 Ad.c.
Max. Short Circuit Current / 最大短路電流 50 Ad.c. per MPPT
AC Output / 交流輸出
Nominal Output Voltage / 額定工作電壓 400 / 380 Va.c.
Nominal Output Frequency / 額定工作頻率 50 / 60 Hz
Connection Type / 連接形式 3Ø3W / 3Ø4W, PE
Max. Continuous Output Current / 最大輸出電流 32 Aa.c.
Rated Continuous Output Power / 額定輸出功率 20000 W
Rated Apparent Output Power / 額定視在功率 20000 VA
Max. Apparent Output Power / 最大視在功率 22000 VA*
Power Factor / 功率因數 0.8 lead ~ 0.8 lag
*20000 VA max for AU/NZ
Protection Class / 保護等級 I
Over Voltage Category / 過電壓類別 III (AC), II (DC)
Ingress Protection / 防護等級 IP66
Operating Temperature Range / 操作溫度範圍 -25 ~ +60℃
Non-isolated inverter 非隔離型變流器
Manufacturing location: Made in China
No. 1688 Jiangxing East Road, Wujiang Economic Development Zone, Suzhou City, 215200 Jiangsu Province,P.R. China
Authorized representative
Delta Electronics (Netherlands) B.V.
Zandsteen 15, 2132 MZ Hoofddorp, The Netherlands
AS 4777.2:2020
IEC 61439-2
E-S,EMC V63595-BSMI
60 sec.