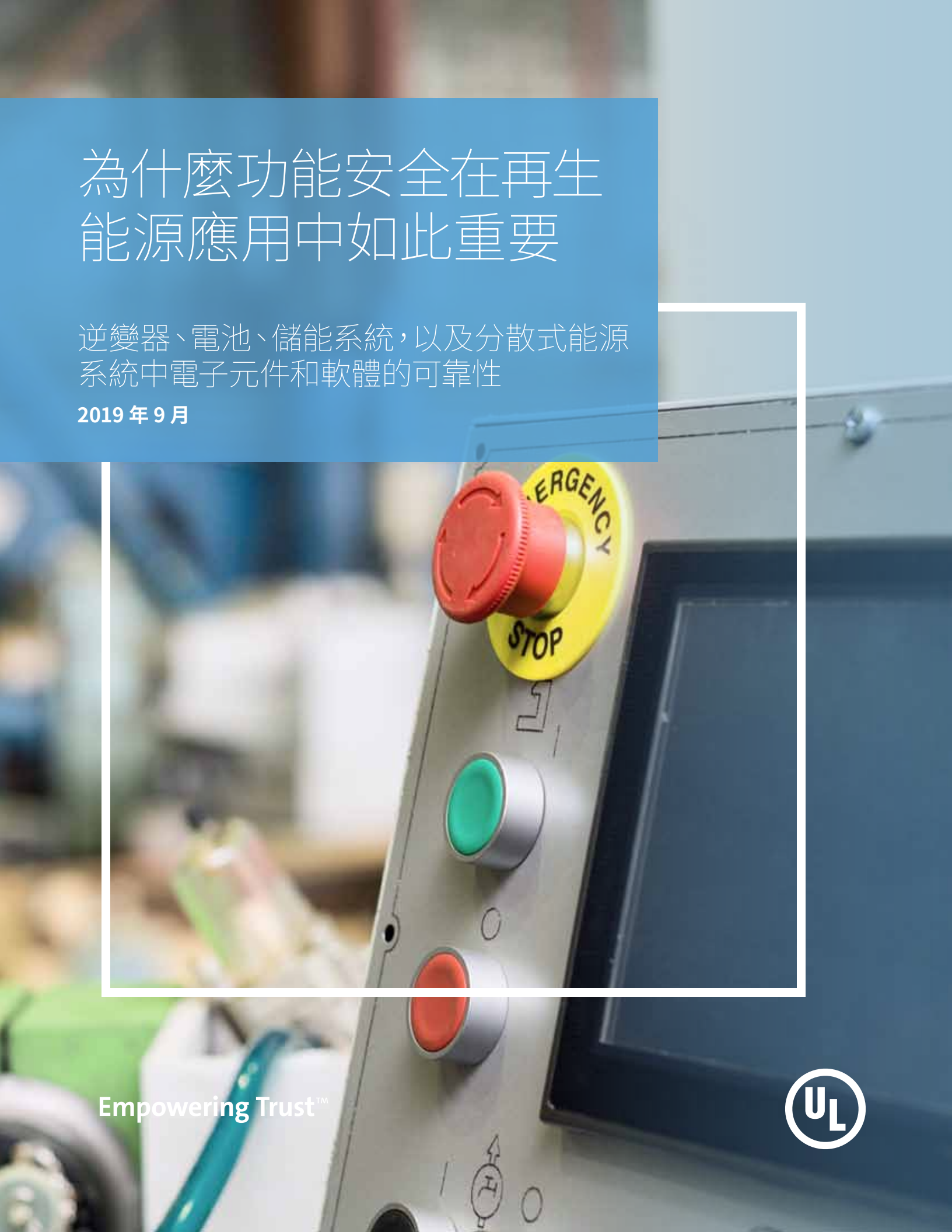
為什麼功能安全在再生能源應用中如此重要

逆變器、電池、儲能系統，以及分散式能源系統中電子元件和軟體的可靠性

2019 年 9 月



Empowering Trust™

Authors

Jason Smith，首席工程師，UL LLC，
諾斯布魯克，伊利諾州 美國

Laurie Florence，首席工程師，UL LLC，
諾斯布魯克，伊利諾州 美國

Timothy P. Zgonena，首席工程師，UL LLC，
諾斯布魯克，伊利諾州 美國

Scott Picco，業務發展經理，能源系統和
電動載具部，UL LLC，諾斯布魯克，
伊利諾州 美國

功能安全

我們都經歷過

當我們購買了一個電動兒童玩具，有一天它卻突然不動了，無論重覆開關電源或是更換電池，都沒有辦法讓它恢復正常運作，這狀況代表的是這個玩具徹底故障了。您或許會生氣地說：“這玩具品質真的不如以往。”

或者，您正使用筆記型電腦編輯一份重要的文件，但是突如其來的當機，也許是因為電腦硬碟或是記憶體故障，導致您遺失了這份文件檔案，浪費了花在處理文件上的時間。

現在試著想像一下，這種內建電子元件卻突然失靈的產品變成了裝有鋰電池的電動滑板車或是正在控制您汽車加速的電腦。倘若這些產品中的電子元件故障了，就不是“不方便”而已，因為您的安全將受到威脅。

但值得慶幸的是，這些故障並不像兒童玩具壞掉或筆記型電腦當機那麼頻繁發生。其中一個主要原因是製造商通常會更小心地確保這些產品中與安全相關的電子元件和軟體的可靠性以及功能性。然而，它們仍然會有潛在的機率在不確定的條件之下發生故障。 [1] [2]

什麼是功能安全?

功能安全的定義就是透過系統評估確保每個主動式保護元件在潛在的隨機性失效風險下都能維持正常運行，以保障整個系統的安全，這個概念稱之為功能安全。常見與功能安全相關的系統產品包括：用來監控鋰離子電池電壓、電流、溫度的電池管理系統，太陽光電的快速切離裝置，車輛上的電子節氣閥門控制系統。

系統功能安全可以透過電子元件、軟體控制、液壓及機械結構等技術手段來達到所需的安全等級。但相關被動式元件，例如保險絲、熱熔斷器、斷路器等被動式元件，即使他們的功用是在於保護整個系統安全的，但通常不需要將該類元件納入功能安全評估規範中，因為被動元件被視為單一保護可靠元件，且被相應的標準規範。

現今，功能安全與電子和軟體的關係變得越來越密切，因為許多原本由液壓或是機械技術實現的功能，因控制晶片的生產技術提升，現在都改由電子迴路搭配軟體技術來取代。然而，這些電子迴路和軟體仍經常出現一些非預期的失效問題，也因此，功能安全評估現在越來越受到人們的重視。

與電子技術和軟體技術相關的問題

任何事物都有可能出現問題，只是出現問題的時間和方式不同。即使設計再完美的產品，經過一段時間的使用，產品的一個或多個元件也會因為外部的環境應力產生一些磨損、老化，導致產品出現故障。一般情況下，產品的平均故障時間是可以被估算的。目前，製造商會根據產品的平均故障時間來制訂產品的品保和維修週期。

現今，電子元件體積越來越小，更加集中化，執行任務的速度也越來越快，正是因為技術的快速發展，讓製造商能夠將各種先進技術封裝在一個小小的元件裡。但也因為這些技術，在一定程度上增加了故障的發生概率，並且縮短了產品的平均故障時間。

系統性失效風險

電子產品中通常會存在一些系統性缺陷，而且有些系統性缺陷在設計上是不可避免的。這些缺陷使得系統可能不會按照預期設計運行。系統性缺陷會導致在同樣情況下所有相同型號的產品出現同樣的問題。因此製造商希望盡可能避免這種類型的缺陷。

系統性缺陷在初始情況下一般不會顯現出來。可能需要一系列條件的組合，例如產品被另一個物體擊中、被閃電擊中、在無線電發射塔旁邊運行或突然斷電，在這些情況下才會出現系統性缺陷導致產品失效。

除此之外，如何避免控制軟體中的系統缺陷，對於開發者來說也是巨大的挑戰。一個程序只有 8 個位元組，不是千位元組、百萬位元組、兆位元組，甚至不足以在你的電腦螢幕上顯示 “Hello World!”，但就可容納18、446、744、073、709、551、616 (18 quintillion) 種可能的組合，其中任一位元發生變化，都有可能導致程序運行後出現不同的結果。

由於這種複雜性，如果存在軟體缺陷(BUG)，那麼程序運行的最終結果將無法預估。另外，還有可能出現這種情況：之前幾次程序運行都沒有問題，但是下一次再運行程序時就出現問題。這種情況發生的主要原因可能是程序的初

始條件發生了變化，例如程序的輸入、定時、環境等改變，導致程序最終運行結果不同，這顯然不是一個隨機事件。

對於上述討論的內容，在進行與安全相關的電子和軟體技術設計時需要審慎考慮。由於電子元件會隨著時間的推移出現磨損、老化，這種磨損、老化帶來的隨機失效無法避免。因此，在設計產品時需要同時考慮隨機失效和系統失效，防止任何失效影響人身安全。

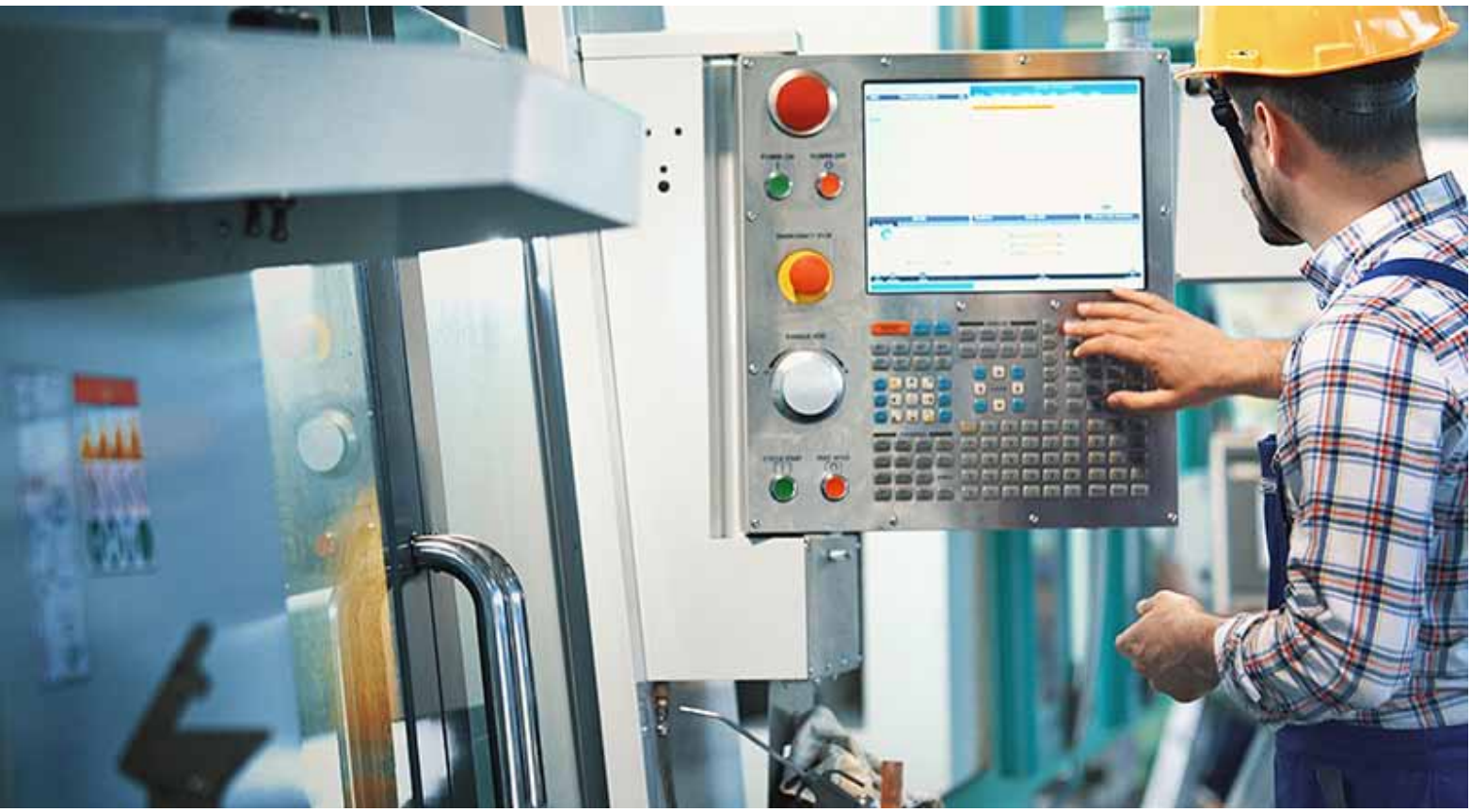
隨機失效風險

前面提及，任何產品都會因為硬體出現磨損、老化而失效。在進行功能安全設計時，最重要的事情之一就是考慮在系統出現隨機失效時的後果。通常，功能安全將失效類型分為三類：失效-危險、失效-安全（關斷），以及失效-運行（故障容錯）。

失效-危險，正如字面上的意思，產品失效後會造成危害，在產品設計中要盡量避免這種失效模式。為了避免這種失效模式，至少需要額外的診斷措施來檢測故障，或是增加冗餘設計來保障系統安全運行。

失效-安全，當檢測到產品失效後系統會被斷開，是安全的，這對於許多與安全相關的基本應用來說已經足夠。這種失效模式也需要在系統中增加額外的診斷措施來檢測故障。例如在程序中增加一個獨立診斷機制去檢測處理器中的快閃記憶體是否存在故障。

但有時候，直接關斷系統並不是一個非常合適的方法。例如在汽車或航空航太領域，當探測到驅動設備中存在故障時，若對驅動設備進行直接關斷，有可能會造成更嚴重的傷害。所以在這種情況下，需要考慮失效-運行這種模式，它指的是即使在系統中存在故障，系統還是處



於安全運行的狀態（維持原有的功能或進行功能降級），透過這種方式來保障人身安全。

失效-運行的系統中至少包含一個冗餘備用的系統，當原有的系統失效時，備用系統能夠取代原有的系統來保障功能的正常運行。這種系統會使系統的元件數量大大增加，因而導致產品的開發成本更高，但是這些額外的成本能夠大大降低系統中存在的隨機性失效風險。

避免系統性缺陷

如上所述，由於電子技術和軟體技術的複雜性，系統性缺陷幾乎無法避免。事實上，歷史上一些最嚴重的電子和軟體故障在本質上都是系統性缺陷導致的。為了減少系統性缺陷的可能性，在功能安全相關的系統設計過程中需要對計畫、實施和測試特別注意。

對於功能安全系統，其研發過程的清晰定義和文檔記錄非常重要。有些人認為這樣只是繁文縟節，但是這些工作能夠迫使開發者進一步思考。同時，將設計寫下來，能夠提供在產品真正生產前，對產品設計進行審查和批准的機會，減少產品存在系統性缺陷。

紀錄設計還能夠進一步讓每個系統中的單元設計目標更清楚，也能夠使系統的測試進行的更加徹底，這對軟體設計非常重要。我們需要確保設計的每一個軟體分支都能夠被測試到，這些設計的軟體單元都能夠按照既定的功能定義運行。

除了正常條件下的測試，功能安全系統的開發還需要進行異常環境條件下的測試，確保在這些條件下還能夠安全運行，如電磁干擾的測試（浪湧、電壓驟降、靜電放電、射頻干擾等），以及一些模擬環境變化的測試（溫濕度、溫度衝擊測試等）。透過這些測試，以證明系統設計的正確性以及能在這些異常條件下安全運行。

在應對一些不可避免的故障時，以上提到的內容是非常具有參考價值的。所有功能安全系統在設計的時候都需要考慮失效-安全和失效-運行兩種模式，而事實上的產品設計並非都如此。例如，波音 737 MAX MCAS 系統，就因為沒有完全遵循這一點而導致了重大的危害事件。[3]

安全認證

UL為成千上萬款的產品提供安全認證服務，其中也包含了那些結合了電子和軟體技術的產品。每一種產品都有它對應的UL標準，這些標準描述了產品需要滿足的安全要求（火災、電氣、機械產生的危險）。UL會透過一些必要的測試對產品進行評估和認證，確保產品滿足了這些安全要求，然後貼附上UL標誌。同時，UL的產品標準還會參考其他適用於該產品的相關標準。

如果產品中的某一零組件與安全有關，那麼該零組件在集成到終端產品前，通常都需要先符合這個零組件的標準要求和測試。考慮到這個特定的零組件和其終端應用，僅僅用終端成品標準來測試該零組件是不夠的，因為終端成品標準並沒有涵蓋所有零組件要考慮的特定關注點。

例如，對保險絲進行 UL248 認證，一般需要根據保險絲的型號和額定等級對保險絲的結構進行評估並且透過測試來驗證熔斷器是否正確可靠地發揮其功能。相較於複雜的電子和軟體應用，保險絲是相對簡單的元件。顯然，如果只是將類似零組件標準的要求應用於電子和軟體就不適當且不足夠。

因此就需要功能安全相關的標準，如 UL991—適用於安全相關的硬體控制設備，和 UL1998—適用於可程式化元件中包含的安全相關軟體。這些標準中包含了對於電子元件和軟體的安全要求，例如需要有合適的診斷機製或者需要冗餘的設計架構，另外對電磁抗干擾也有相關要求，還提到了關於產品應對嚴苛環境條件的穩定性要求。

在某些有限的情況下，允許將電子和軟體進行黑盒子測試評估，也就是說，只考慮終端產品的標準要求而不考慮功能安全的要求。但是這不能夠保證，當產品離開生產線後或失效之後還能夠安全地運行。此外，軟體需要頻繁的更新和升級，在這種情況下黑盒子的測試方法就不適用。但是，據了解，有一些獲國家認可的測試實驗室 (NRTLs) 仍不適當地將此功能安全黑盒子測試方法擴展到所有設備。這顯然是不被允許的，任何允許使用黑盒子方法的產品都會在其特定的產品標準中進行明確說明。

支援智慧電網和併聯型逆變器、太陽光電 / 太陽能系統以及分散式能源 (DER) 設備的功能安全問題

現代併網逆變器包含了功率變換、高速運算、實時電能計量和分析、通訊以及輸入和輸出電路控制功能，同時還可當作太陽光電系統的安全監視器來防止各種電擊、火災和高能量相關的危害。太陽能和分散式能源產業是近年越來越依賴逆變器功能的極佳例子，太陽能逆變器所承擔的責任也越來越多。逆變器已經成為太陽能/分散式能源系統的大腦，而軟體則是其最關鍵的零組件。

逆變器提供整個太陽能和微電網系統越來越多的保護和功能。美國國家電氣規範 (NEC) 要求設備所執行的功能符合適用的安全標準。最近NEC、安全標準以及支併網和電網支援標準的變化將直接影響逆變器認證。了解這些標準和規範相當重要，有助於正確應用所設計、製造、認證和安裝的設備。

功能安全適用領域包括但不限於:

- 過電流保護和電源控制系統 (PCS) 電流監測和限制功能 (2020 版 NEC) 。
- 太陽光電系統保護：接地故障、電弧故障、太陽光電快速關斷設備和系統，包括未來 UL3741 標準中的太陽光電危害控制。
- 交流模組、交流模組系統以及安裝在太陽

光電模組上用於智慧接線盒的電子設備。

- 用於儲能系統(ESS)，並與電池管理系統(BMS)設備的配合使用。

相關的功能安全標準有：

UL 標準	UL 標準名稱
UL 1741	用於分散式電源的逆變器、變流器、控制器和互聯系統設備的標準
UL 62109	太陽能電力系統中使用的電力變流器的安全標準
UL 3741	太陽光電危害控制的標準
UL 1699B	太陽光電 (PV) 直流電弧故障電路保護標準
UL 2231 (參考UL 2202)	電動汽車 (EV) 供電電路的人員保護系統的安全標準：充電系統中使用的保護裝置的特殊要求
UL 2200	固定式引擎發電機元件標準

逆變器是微電網和複合型（併網+離網）應用的關鍵組件。為維護分散式能源系統的安全可靠，硬體、韌體和軟體的可靠性（包括互聯網連接、通信、遠程修改和網路安全）將是關鍵的考慮因素。

可編程電子元件已經成為分散式發電和再生能源系統的發電、控制和保護電路的通用基礎。可程式化電子產品的成長和擴展不斷取代單個分離式的電子控制和保護元件。轉換使用可編程電子元件的過程也允許整體功能的組合和整合。可靠度的重要性，並進一步說明了功能安全評估的重要性。

幸運的是，這個產業能夠利用已發布的功能安全標準來進行評估，其中明確定義了評估電子控制和可編程電子設備的功能和可靠性的方法。本產業使用的主要功能安全標準是：

UL 標準	UL 標準名稱
UL 60730	電氣自動控制安全標準
UL 1998	可編程元件軟體標準
UL 991	使用固態裝置的安全相關控制裝置的安全測試標準

所有美國或 UL 再生能源和分散式能源的安全標準都明確要求安全關鍵電子控制、軟體或可編程電子特性和功能的評估，並符合這些功能安全標準。

由保護電路失效引起的故障模式（電擊、危險能量或火災）的嚴重性，是這些再生能源和分散式能源標準中功能安全要求的主要驅動因素。環境應力和電氣可靠性測試對這些關鍵軟硬體功能的可靠性和安全性有著非常重要的維護作用。故障模式失效影響分析（FMEA）有助於確保除了應力測試，這些電路在單一故障下是安全的。如果不進行功能安全調查，設備或系統安全運行的可靠性可能會受到損害。

小型和大型電池儲能和儲能系統的功能安全問題

依靠電池儲存能量的儲能系統使用電子和軟體進行安全監測和關鍵安全控制。例如，鋰離子電池需要在其安全工作區域內進行充電和放電。電池工作過程中的電流、電壓和溫度參數不應超出鋰離子電池製造商規定的電池充放電工作區域，否則可能造成嚴重的安全隱憂。

這尤其適用於充電電壓限值，該限值與溫度有關，必須嚴格控制，若沒有電池管理系統 (BMS) 就無法實現這一級別的控制，電池管理系統本質上是一個可編程的電子控制板，用於監測和控制電池系統的運行。由於電池管理系統對儲能系統的安全運行相當重要，因此必須徹底分析電池管理系統和電池，對儲能電池管理系統進行功能安全調查，評估其可靠性。電池管理系統應在電池的整個使用壽命內按預期保護電池，並能在預期的環境應力範圍內可靠運行。電池管理系統應具有足夠的冗餘保護，以確保其運行的可靠性，進而將系統維持在安全狀態。

為了確保電池儲能系統的控制功能依預期運行，並在系統使用壽命內具有一定的可靠性，電池管理系統必須進行功能安全評估。該評估應基於徹底的安全分析，如故障模式失效影響分析（FMEA），其中確認與安全高度相關的電子元件和軟體，須依據適當的功能安全標準進行評估。評估應包括關鍵安全功能的冗餘，及對環境影響的的防護能力，包括電磁相容性 EMC、環境溫度和其他可能影響電池系統運行及其安全控制的因素。

儲能系統需要的功能安全評估標準有：

UL 標準	UL 標準名稱
UL 1973	固定設備用電池、車用輔助電池和輕型軌道交通用電池標準
UL 9540	儲能系統和設備的標準
UL 2271	輕型電動車用電池標準
UL 2580	電動汽車用電池標準
UL 2849	電動自行車、電動輔助自行車、電動車和電動摩托車標準
UL 2272	個人行動設備的電氣系統標準

在對系統進行安全分析時，沒有任何捷徑，要充分了解系統的安全需求、以及用來維繫安全的控制能力，這對於防止現場發生安全事故相當重要。電池儲能系統的安全控制不足可能會導致安全事故的發生，包括起火和鋰電池的熱失控引起的爆炸，進而導致整個電池系統的連鎖反應。簡而言之，在電池的功能方面是不允許有黑盒子評估結果的存在。

例如，鋰電池充電時，哪怕超過充電電壓上限 1V，也會導致電池過壓充電，進而導致電池失效並可能引發熱失控。電池管理系統會一直監控電池的溫度和電壓等參數，當電池的這些參數達到極限時，BMS 就會做出反應，降低或停

止對電池的充放電，以防止發生危險。電池管理系統是電池儲能系統的關鍵安全零組件，對電池管理系統進行功能安全評估是確保儲能系統的電池管理系統能夠按照設計的情況正常運行的關鍵。

在更加複雜的電池儲能系統中，可能會有一個額外的能量管理系統來控制多個電池系統、電池管理系統、以及影響系統整體安全性的其他零組件，對電池管理系統進行的安全分析同樣也擴展到能源管理系統 (EMS)。與電池管理系統類似，能源管理系統由可編程的電子控制板組成，以確保電池儲能系統的所有元件可以共同工作，以免超出其相應的規格，如果超出其相應規格就可能會發生危險。一個具有多個電池系統的大型儲能系統所包含的能量非常值得我們關注。一個電池系統內的火災可以蔓延到整個儲能系統，導致重大火災。最開始的火災進一步蔓延後，會導致可燃氣體的釋放和潛在的爆炸，甚至對建築物和周圍地區構成火災和爆炸的威脅。

EMS分析時需要考慮影響其安全性的所有零組件和軟體，並且需要考慮通信系統的可靠性，而通信系統可以被視為是整個系統安全方案的一部分。如果沒有可靠的控制來監測和確保儲能系統的安全運行，系統就不能對運行過程中可能出現的異常情況做出可靠的反應。對儲能系統的控制進行安全分析和功能安全評估是確保大型複雜的儲能系統可以在其預期的壽命內安全運行的關鍵。

如果對電池儲能系統沒有進行嚴格的安全分析、適當級別的功能安全評估和測試，那麼電池或儲能系統的維護人員、用戶和附近人員遭受火災和電擊的風險就會顯著增加，比如說電池和儲能系統所在的建築就會處於危險之中。這種失控情況會導致附近更大區域的財產和人員損失害。

如需向UL專家了解更多功能安全在再生能源中的應用，請聯繫:
renewableenergyquote@ul.com

參考資料

[1] https://www.cpsc.gov/Safety-Education/Safety-Education-Centers/hoverboards

[2] https://www.eetimes.com/document.asp?doc_id=1323061

[3] https://www.seattletimes.com/business/boeing-aerospace/a-lack-of-redundancies-on-737-max-system-has-baffled-even-those-who-worked-on-the-jet/

UL.com

210.01.1219.CN.EPT