



(19)中華民國智慧財產局

(12)發明說明書公告本

(11)證書號數：TW I569164 B

(45)公告日：中華民國 106 (2017) 年 02 月 01 日

(21)申請案號：102102670

(22)申請日：中華民國 102 (2013) 年 01 月 24 日

(51)Int. Cl. : G06F21/50 (2013.01)

G06F21/60 (2013.01)

(30)優先權：2012/02/08 美國

13/368,419

2012/10/01 英國

1217531.1

2012/11/19 英國

1220771.8

(71)申請人：A R M股份有限公司(英國) ARM LIMITED (GB)

英國

(72)發明人：格羅卡特湯瑪士克里斯多夫 GROCUTT, THOMAS CHRISTOPHER (GB)；格利森

斯維特理查羅伊 GRIENTHWAITE, RICHARD ROY (GB)

(74)代理人：蔡坤財；李世章

(56)參考文獻：

TW 201102929A

US 2004/0139346A1

US 2011/0225402A1

ARM Limited, Cortex-M3, Revision: r1p1, Technical Reference

Manual, 2006, ARM Limited, downloaded from [http://](http://infocenter.arm.com/help/topic/com.arm.doc.ddi0337c/DDI0337E-cortex-m3-r1p1-trm.pdf)[infocenter.arm.com/help/topic/com.arm.doc.ddi0337c/DDI0337E-](http://infocenter.arm.com/help/topic/com.arm.doc.ddi0337c/DDI0337E-cortex-m3-r1p1-trm.pdf)[cortex-m3-r1p1-trm.pdf](http://infocenter.arm.com/help/topic/com.arm.doc.ddi0337c/DDI0337E-cortex-m3-r1p1-trm.pdf)

審查人員：高嘉男

申請專利範圍項數：19 項 圖式數：13 共 65 頁

(54)名稱

在具有安全網域與較不安全網域之資料處理設備之例外處理

EXCEPTION HANDLING IN A DATA PROCESSING APPARATUS HAVING A SECURE DOMAIN AND A LESS SECURE DOMAIN

(57)摘要

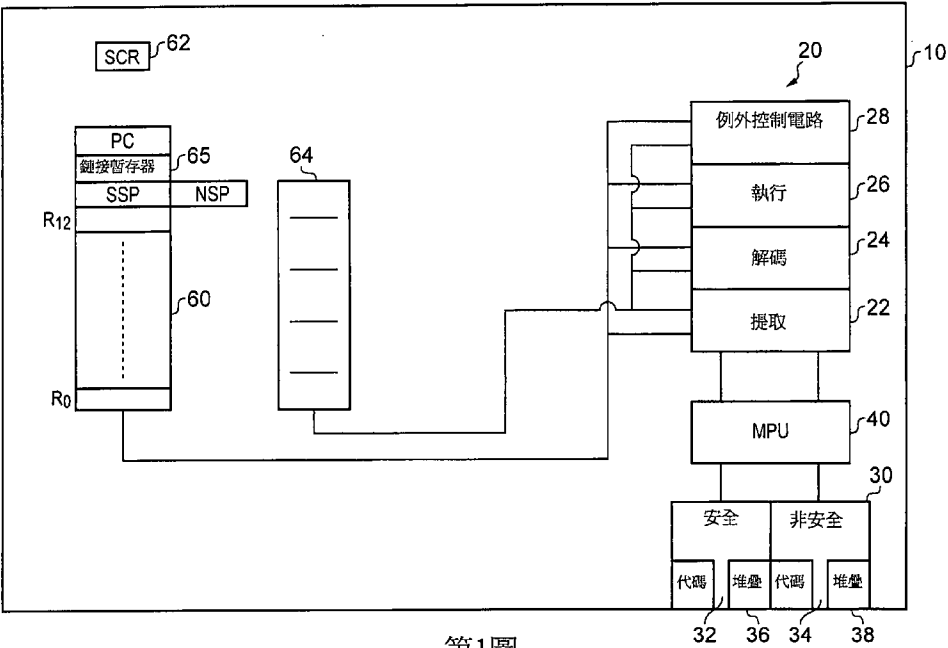
本發明提供一種用於處理例外之資料處理設備及方法，該資料處理設備具有經配置以回應於程式碼執行資料處理操作之處理電路，該處理電路包含用於控制例外處理之例外控制電路。提供複數個暫存器以儲存資料，該等暫存器包括第一子集之暫存器及第二子集之暫存器，且亦提供資料儲存器以儲存資料，該資料儲存器包含複數個區域，該複數個區域包括安全區域及較不安全區域，其中該安全區域係用於儲存當操作於安全網域中時處理電路可存取，且當操作於較不安全網域中時處理電路不可存取之資料。回應於來自處理電路執行之背景處理的初始例外，例外控制電路在觸發處理電路執行對應於該例外之例外處理常式之前執行來自第一子集之暫存器的資料之狀態保存，其中該例外處理常式具有執行來自第二子集之暫存器之資料的狀態保存之責任。回應於引起自安全網域至較不安全網域之轉變的第一例外，其中背景處理係藉由處理電路在安全網域中執行，例外控制電路在觸發處理電路執行在較不安全網域中之例外處理常式之前執行來自第二子集之暫存器之資料的額外狀態保存。本發明之硬體機制在不需要經由例外處理程式代理之情況下賦能安全例外之有效處理。

A data processing apparatus and method are provided for handling exceptions, the data processing apparatus having processing circuitry configured to perform data processing operations in response to program code, the processing circuitry comprising exception control circuitry for controlling exception processing. A plurality of registers are provided to store data, the registers including a first subset of registers and a second subset of registers, and a data store is also provided to store data, the data store comprising a plurality of regions including a secure region and a less secure region, wherein the secure region is for storing data which is accessible by the processing circuitry when operating in a secure domain and not accessible by the processing circuitry when operating in a less secure domain. In response to an initial exception from background processing performed by the processing circuitry, the exception control circuitry performs state saving of data from the first subset of registers before triggering the processing circuitry to perform an exception handling routine corresponding to the exception, wherein the exception handling routine has responsibility for performing state saving of data from the second subset of registers. In response to a first exception causing a transition from the secure domain to the less secure domain, where the background processing was performed by the processing circuitry in the secure domain, the exception control circuitry performs additional state saving of the data from the second subset of registers before triggering the processing circuitry to perform the exception handling routine in the less secure domain. The hardware mechanism of the present invention enables effective handling of secure exceptions without requiring proxying through an exception handler.

指定代表圖：

符號簡單說明：

- 10 . . . 資料處理設備
- 20 . . . 處理電路
- 22 . . . 提取電路
- 24 . . . 解碼電路
- 26 . . . 執行電路
- 28 . . . 例外控制電路
- 30 . . . 資料儲存器
- 32 . . . 安全區域
- 34 . . . 非安全區域
- 36 . . . 安全堆疊
- 38 . . . 非安全堆疊
- 40 . . . 記憶體保護單元
- 60 . . . 暫存器組
- 62 . . . 安全配置暫存器
- 64 . . . 額外暫存器組



第1圖

65 . . . 鏈接暫存器
R0 . . . 值
R12 . . . 值

發明摘要

※ 申請案號：102102670

※ 申請日：102 年 1 月 24 日

※IPC 分類：G06F 21/50 (2013.01)
G06F 21/60 (2013.01)

【發明名稱】（中文/英文）

在具有安全網域與較不安全網域之資料處理設備之例外處理

**EXCEPTION HANDLING IN A DATA PROCESSING
APPARATUS HAVING A SECURE DOMAIN AND A
LESS SECURE DOMAIN**

【中文】

本發明提供一種用於處理例外之資料處理設備及方法，該資料處理設備具有經配置以回應於程式碼執行資料處理操作之處理電路，該處理電路包含用於控制例外處理之例外控制電路。提供複數個暫存器以儲存資料，該等暫存器包括第一子集之暫存器及第二子集之暫存器，且亦提供資料儲存器以儲存資料，該資料儲存器包含複數個區域，該複數個區域包括安全區域及較不安全區域，其中該安全區域係用於儲存當操作於安全網域中時處理電路可存取，且當操作於較不安全網域中時處理電路不可存取之資料。回應於來自由處理電路執行之背景處理的初始例外，例外控制電路在觸發處理電路執行對應於該例外之例外處理常式之前執行來自第一子集之暫存器的資料之狀態保存，其中該例外處理常式具有執行來自

第二子集之暫存器之資料的狀態保存之責任。回應於引起自安全網域至較不安全網域之轉變的第一例外，其中背景處理係藉由處理電路在安全網域中執行，例外控制電路在觸發處理電路執行在較不安全網域中之例外處理常式之前執行來自第二子集之暫存器之資料的額外狀態保存。本發明之硬體機制在不需要經由例外處理程式代理之情況下賦能安全例外之有效處理。

【英文】

A data processing apparatus and method are provided for handling exceptions, the data processing apparatus having processing circuitry configured to perform data processing operations in response to program code, the processing circuitry comprising exception control circuitry for controlling exception processing. A plurality of registers are provided to store data, the registers including a first subset of registers and a second subset of registers, and a data store is also provided to store data, the data store comprising a plurality of regions including a secure region and a less secure region, wherein the secure region is for storing data which is accessible by the processing circuitry when operating in a secure domain and not accessible by the processing circuitry when operating in a less secure domain. In response to an initial exception from background processing performed by the processing

circuitry, the exception control circuitry performs state saving of data from the first subset of registers before triggering the processing circuitry to perform an exception handling routine corresponding to the exception, wherein the exception handling routine has responsibility for performing state saving of data from the second subset of registers. In response to a first exception causing a transition from the secure domain to the less secure domain, where the background processing was performed by the processing circuitry in the secure domain, the exception control circuitry performs additional state saving of the data from the second subset of registers before triggering the processing circuitry to perform the exception handling routine in the less secure domain. The hardware mechanism of the present invention enables effective handling of secure exceptions without requiring proxying through an exception handler.

【代表圖】

【本案指定代表圖】：第（ 1 ）圖。

【本代表圖之符號簡單說明】：

- 10 資料處理設備
- 20 處理電路
- 22 提取電路
- 24 解碼電路

26	執行電路
28	例外控制電路
30	資料儲存器
32	安全區域
34	非安全區域
36	安全堆疊
38	非安全堆疊
40	記憶體保護單元
60	暫存器組
62	安全配置暫存器
64	額外暫存器組
65	鏈接暫存器
R0	值
R12	值

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

無

發明專利說明書

(本說明書格式、順序，請勿任意更動)

【發明名稱】(中文/英文)

在具有安全網域與較不安全網域之資料處理設備之例外處理

EXCEPTION HANDLING IN A DATA PROCESSING APPARATUS HAVING A SECURE DOMAIN AND A LESS SECURE DOMAIN

【技術領域】

【0001】本發明之技術領域係關於資料處理之領域，且更特定言之，係關於敏感資料及代碼之處理。

【先前技術】

【0002】許多資料處理系統及架構提供隔離及保護敏感資料及代碼區段，以免由未授權人員或程序存取之方法。儘管能夠提供安全性很重要，但是在與此保護相關聯之效能及電路區域中存在額外負擔。

【0003】在諸如微控制器之較小系統中，將該等額外負擔保持較低非常重要，且因此可能需要進行安全位準與效能之間的一些折衷。

【0004】保持資料及代碼安全之一種方式係藉由 Cambridge UK 之 ARM®提供，Cambridge UK 之 ARM®具有其中存在安全狀態及非安全狀態（亦稱為安全網域及非安全網域）之 Trustzone 架構，且使用例外指令在該等狀態之間轉

變，該例外處理程式保護安全側之安全性。儘管此方法提供高度安全性，但是需要以軟體例外處理程式形式之可觀之軟體介入來改變安全狀態，如此降低了系統之效能且增加了為安全軟體開發外部應用程式介面 API 所需之工作量，因為所有調用皆必須經由例外處理程式代理。類似地，當在安全網域中時發生之需要非安全網域中之處理的例外亦需要經由安全例外處理程式代理，如此允許安全狀態在控制傳遞至非安全例外處理程式之前得以保護。

【0005】 US7966466 及 US 2008/0250216 揭示了其中資料儲存器具有安全側及非安全側之替代安全系統，且在當前被執行之代碼的該資料儲存器之內的位置決定處理器正操作於其中之網域，且因此決定允許存取之資料。

【發明內容】

【0006】 自第一態樣來看，本發明提供一種資料處理設備，該資料處理設備包含：處理電路，該處理電路經配置以回應於程式碼執行資料處理操作，該處理電路包含用於控制例外處理之例外控制電路；複數個暫存器，該複數個暫存器經配置以儲存資料，該等暫存器包括第一子集之暫存器及第二子集之暫存器；及經配置以儲存資料之資料儲存器，該資料儲存器包含複數個區域，該複數個區域包括安全區域及較不安全區域，其中安全區域係用於儲存當操作於安全網域中時處理電路可存取，且當操作於較不安全網域中時處理電路不可存取之資料；其中：回應於來自由處理電路執行之背景處理之初始例外，例外控制電路經配置以在觸發處理電路執

行對應於例外之例外處理常式之前執行來自第一子集之暫存器之資料的狀態保存，其中例外處理常式具有執行來自第二子集之暫存器之資料的狀態保存的責任；且回應於引起自安全網域至較不安全網域之轉變的第一例外，其中背景處理係藉由處理電路在安全網域中執行，例外控制電路經配置以在觸發處理電路執行較不安全網域中之例外處理常式之前執行來自第二子集之暫存器的資料之額外狀態保存。

【0007】當在背景處理期間發生例外時，背景處理可能已將資料值置放於暫存器中，且因此允許當例外完成時保留且恢復該等資料值，系統可執行來自暫存器之資料至資料儲存器（通常保存至提供於資料儲存器中之堆疊）之狀態保存。如上文論述，對於某些系統，重要的是在所達成之安全位準與處理效能之間達成折衷。當回應於例外執行狀態保存時亦是如此。

【0008】由於效能原因，執行第一子集及第二子集中之暫存器中的資料之狀態保存可能是有用的。根據本發明，來自第一子集之資料的狀態保存可在觸發例外處理常式之前藉由硬體中之例外控制電路執行。相反，例外處理常式（亦即，軟體）可具有執行來自第二子集之暫存器之資料的狀態保存的責任。

【0009】然而，自安全性角度來看，在例外處理常式之控制下的第二子集之暫存器之狀態保存有時可能是有問題的。若在安全網域中執行之背景處理後，例外引起自安全網域至較不安全網域之轉變，則例外處理常式在安全網域中時可修

改置放於第二子集之暫存器中之安全資料。

【0010】根據本發明，爲了防止此安全破壞，若發生引起自安全網域至較不安全（在本文中亦稱爲非安全）網域之轉變（其中背景處理處於安全網域中）的第一例外，則例外控制電路在觸發在較不安全網域中之例外處理常式之前，執行來自除第一子集之暫存器之外的第二子集之暫存器的資料之額外狀態保存。藉由提供用於在觸發例外處理常式之前保存第二子集之暫存器之狀態的硬體機制，可以防止軟體在較不安全網域中對此資料的修改。

【0011】因此，當回應於例外執行狀態保存時，本發明技術可在安全性與效能之間達成改良之平衡。本發明之硬體機制在不需要經由安全例外處理程式代理之情況下賦能較不安全例外之有效處理。

【0012】回應於第一例外，在一個實施例中之例外控制電路經配置以在觸發處理電路執行例外處理常式之前清空第二子集之暫存器。如此意謂在較不安全網域中之例外處理常式在安全網域中時無法存取置放於第二子集之暫存器中之任何資料。

【0013】進一步地，在一個實施例中，回應於該第一例外，資料處理設備經配置以確保在例外控制電路觸發處理電路執行例外處理常式之前，第一子集之暫存器不含有安全資料。存在可以達成此舉之多個方式。例如，硬體或軟體可確保清空了第一子集之暫存器，使得彼等暫存器不含有任何安全資料。或者，情況可能是在觸發處理電路執行例外處理常

式之前，可設計第一子集之暫存器以便僅包括非安全資料，在該情況下，可能不必清空第一子集之暫存器。

【0014】在本申請案中，術語「調用者暫存器」及「被調用者暫存器」可用以分別指示第一子集之暫存器及第二子集之暫存器。

【0015】雖然例外處理常式具有執行來自第二子集之暫存器（被調用者暫存器）之資料之狀態保存的責任，但是例外處理常式實際上執行來自第二子集之資料的狀態保存並不總是必要的。例如，若例外控制電路已執行第二子集之暫存器的額外狀態保存，則例外處理常式可忽略該等暫存器之狀態保存。

【0016】或者，例外處理常式總是執行來自被調用者暫存器之資料的狀態保存可能是較為簡單的，即使已藉由硬體進行額外狀態保存。由於暫存器可能已藉由硬體清空，所以例外處理常式將不會以任何方式存取先前保持於被調用者暫存器中之任何安全資料值，且與保存經清空之資料值至資料儲存器之較不安全區域且稍後恢復經清空之資料值相關聯之額外負擔（當例外完成時）可小於與提供一機制相關聯之額外負擔，該機制用於允許例外處理常式偵測是否硬體已執行額外狀態保存。

【0017】關於第一子集之暫存器（調用者暫存器）及第二子集之暫存器（被調用者暫存器），在一個實施例中，第一子集之暫存器有可能包含零個暫存器，使得需要保持在例外處理程式周圍之所有暫存器皆在第二子集中。在此情況下，

對於無狀態保存由例外控制電路執行之大部分例外，其中例外處理常式具有保存在第二子集中之所有暫存器的責任。然而，回應於引起自安全網域至較不安全網域之轉變的第一例外，額外狀態保存可使用例外控制電路將第二子集（需要保持之所有暫存器）保存在硬體中，以防止藉由較不安全網域中之例外處理常式對此資料之存取。

【0018】進一步例外待在当前例外已完成之時待決是可能的。在此情況下，處理電路可在返回至背景處理之前服務於該進一步例外，在当前例外之前正執行該背景處理。此情況被稱為「尾鏈」，且進一步例外稱為「尾鏈」例外。

【0019】觸發額外狀態保存之第一例外可為初始例外，該初始例外在處理電路正執行背景處理時發生。或者，第一例外自身可為尾鏈例外，該尾鏈例外在初始例外之後但在返回至背景處理之前得以處理。

【0020】在本申請案中，術語「背景處理」可用於指示由具有較高優先級之例外中斷之處理。若例外處理常式自身係由較高優先級例外（在本文中稱為搶先例外）中斷，則被中斷之例外處理常式自身可成為搶先例外之「背景處理」，且該搶先例外隨後可在中斷之前觸發由例外處理常式使用之資料之狀態保存。

【0021】在使用尾鏈之一個實施例中，有可能降低結合尾鏈例外所需之狀態保存量。特定言之，在一個實施例中，回應於具有比當前例外低之優先級的新例外，該當前例外之相應例外處理常式仍正在執行，例外控制電路經配置以在引起

處理電路返回至背景處理之前將新例外之處理作為尾鏈例外來控制。進一步，例外控制電路經配置以當控制新例外之處理時不執行進一步狀態保存操作，除非出現下列情況之一：該當前例外在該安全網域中執行，該新例外指示切換至該較不安全網域，及該背景處理係在該安全網域中執行，此時該例外控制電路經配置以在完成該當前例外之例外處理常式之後，執行來自該第二子集之暫存器之資料的該額外狀態保存，且確保在觸發處理電路執行對應於新例外之例外處理常式之前清空該第二子集之暫存器。如上所述，第一子集之暫存器的清空可能必須或可能不必依賴於實施。該方法允許當非安全尾鏈例外跟隨安全例外時資料之安全性得以保持，該安全例外自身引起安全背景處理中之中斷。

【0022】 當處理尾鏈例外時亦可進行關於狀態恢復操作之進一步效率。例如，在一個實施例中，例外控制電路經配置以當控制新例外之處理時不執行狀態恢復操作，除非出現下列情況之一：該當前例外在該較不安全網域中執行，該新例外指示切換至該安全網域，及該背景處理係在該安全網域中執行；此時該例外控制電路經配置以在完成該當前例外之例外處理常式之後，在觸發處理電路執行對應於新例外之例外處理常式之前執行資料之狀態恢復操作至該第二子集之暫存器中。

【0023】 如上所述，將在當前例外正在處理時發生之較高優先級例外處理為搶先例外。若該搶先例外在處理當前例外中之早期發生，且特定言之當在觸發處理電路執行當前例外

之例外處理常式之前，例外控制電路仍然正在處理上文所述之狀態保存操作或額外狀態保存操作時，則可在一個實施例中修改例外控制電路之狀態保存操作及額外狀態保存操作。特定言之，在一個實施例中，若在執行第二子集之暫存器之額外狀態保存時發生具有比該第一例外高之優先級的搶先例外，且該搶先例外不需要自安全網域至較不安全網域之轉變，則例外控制電路經配置以在觸發處理電路處理搶先例外之例外處理常式之前將額外狀態保存反向。

● **【0024】** 或者或另外，若當前例外不引起自安全網域至較不安全網域之轉變，且若在與當前例外相關聯之例外處理常式的處理開始之前發生搶先例外，該搶先例外具有比當前例外高之優先級且需要自安全網域至較不安全網域之轉變，則例外控制電路可經配置以在觸發處理電路處理搶先例外之例外處理常式之前另外地執行來自第二子集之暫存器的資料之額外狀態保存。

● **【0025】** 若在例外控制電路已執行關於當前例外之任何所需狀態保存或額外狀態保存之後發生搶先例外，且已觸發處理電路執行彼當前例外之例外處理常式，但該搶先例外在彼例外處理常式已完成之前發生，則在一個實施例中，該例外控制電路經配置以當決定在觸發處理電路執行搶先例外之例外處理常式之前，是否需要該第一子集之暫存器之該狀態保存，或該第一子集及第二子集之暫存器之該狀態保存時，將當前例外作為該背景處理來處理。

【0026】 在一個實施例中，資料儲存器包含複數個堆疊，

該複數個堆疊包括在安全區域中之安全堆疊，及在較不安全區域中之較不安全堆疊。在該等實施例中，當執行來自第一子集之暫存器的資料之狀態保存及來自第二子集之暫存器的資料之額外狀態保存時，例外控制電路經配置以將資料保存至安全堆疊及較不安全堆疊中之一者，該安全堆疊及較不安全堆疊中之一者對應於網域之安全性，當執行該背景處理時處理電路在該網域中操作。

【0027】在一個實施例中，資料處理設備進一步包含用於儲存安全配置值之安全配置儲存位置，該安全配置值指示該複數個暫存器中之哪些暫存器係可藉由當前執行之代碼用於儲存安全資料，其中回應於引起自安全網域至較不安全網域之轉變的例外，例外控制電路經配置以在該第二子集之暫存器之內包括由該安全配置值指示之該等暫存器中之一或更多個暫存器。因此，如此允許關於形成至少第二子集之暫存器之暫存器的一些可配置性，由此允許關於哪些暫存器經受由例外控制電路執行之額外狀態保存操作的一些可配置性。

【0028】在一個實施例中，資料處理設備進一步包含用於儲存例外返回値之儲存位置，該處理電路經配置以在該例外返回値之內設定網域值，以指示該資料處理設備在自該背景處理獲得初始例外時操作所處之網域，該例外控制電路依賴於該網域值決定該等暫存器中之哪些暫存器應進行狀態保存操作或狀態恢復操作。如此提供用於允許例外控制電路決定在任何特定情況下是否需要狀態保存及/或額外狀態保存之簡單機制。

【0029】自第二態樣來看，本發明提供一種資料處理設備，該資料處理設備包含：資料處理電路，該資料處理電路用於回應於程式碼執行資料處理操作；複數個暫存器；及用於儲存資料之資料儲存器，該資料儲存器包含複數個區域，每一區域具有安全位準，且該資料儲存器包含至少一個安全區域及較不安全區域，該安全區域用於儲存由操作於該安全網域中之該資料處理電路可存取且由操作於較不安全網域中之該資料處理電路不可存取的敏感資料，該較不安全區域用於儲存較不安全資料；該資料儲存器包含至少至少兩個堆疊：在該安全區域中之安全堆疊，及在該較不安全區域中之較不安全堆疊；其中該資料處理電路包含例外處理電路，該例外處理電路經配置以當該資料處理電路正在該安全網域中執行時回應於例外之接收，且該例外指示切換以執行在較不安全網域中之程式碼以清空一組該等暫存器，在該組該等暫存器之內的該等暫存器取決於該執行網域之安全位準以及待在其中獲得該例外之該網域。

【0030】在一個該實施例中，資料處理電路進一步經配置以將儲存於該組該等暫存器中之狀態保存至該網域之該堆疊，該資料處理電路在清空該組該等暫存器之前執行於該網域中。

【0031】此外，在一個實施例中，資料處理設備包含用於儲存值之安全配置儲存位置，該值指示該複數個暫存器中之哪些暫存器可藉由當前執行代碼用於儲存安全狀態，該資料處理電路經配置以依賴於由該安全配置值指示之該複數個暫

存器及該執行網域之安全位準，以及待在其中獲得該例外之該網域，決定哪些暫存器在該組暫存器之內。

【0032】自第三態樣來看，本發明提供一種在資料處理設備上處理資料之方法，該資料處理設備包含：處理電路，該處理電路用於回應於程式碼執行資料處理操作，該處理電路包含用於控制例外處理之例外控制電路；用於儲存資料之複數個暫存器，該等暫存器包括第一子集之暫存器及第二子集之暫存器；及用於儲存資料之資料儲存器，該資料儲存器包含複數個區域，該複數個區域包括安全區域及較不安全區域，其中該安全區域係用於儲存當操作於安全網域中時處理電路可存取，且當操作於較不安全網域中時處理電路不可存取之資料；該方法包含以下步驟：回應於來自由處理電路執行之背景處理的初始例外，使用例外控制電路以在觸發處理電路執行對應於例外之例外處理常式之前執行來自第一子集之暫存器的資料之狀態保存，其中例外處理常式具有執行來自第二子集之暫存器的資料之狀態保存之責任；及回應於引起自安全網域至較不安全網域之轉變的第一例外，其中背景處理係藉由處理電路在安全網域中執行，使用例外控制電路以在觸發處理電路執行在較不安全網域中之例外處理常式之前，執行來自第二子集之暫存器的資料之額外狀態保存。

【0033】自第四態樣來看，本發明提供一種資料處理設備，該資料處理設備包含：用於回應於程式碼執行資料處理操作的處理手段，該處理手段包含用於控制例外處理之例外控制手段；用於儲存資料之複數個暫存器手段，該複數個暫

存器手段包括第一子集之暫存器手段及第二子集之暫存器手段；及用於儲存資料之資料儲存器手段，該資料儲存器手段包含複數個區域，該複數個區域包括安全區域及較不安全區域，其中該安全區域係用於儲存當操作於安全網域中時處理手段可存取，且當操作於較不安全網域中時處理手段不可存取之資料；其中：回應於來自由處理手段執行之背景處理的初始例外，例外控制手段在觸發處理手段執行對應於該例外之例外處理常式之前執行來自第一子集之暫存器手段的資料之狀態保存，其中例外處理常式具有執行來自第二子集之暫存器手段的資料之狀態保存之責任；及回應於引起自安全網域至較不安全網域之轉變的第一例外，其中背景處理係藉由處理手段在安全網域中執行，例外控制手段在觸發處理手段執行在較不安全網域中之例外處理常式之前，執行來自第二子集之暫存器手段的資料之額外狀態保存。

【圖式簡單說明】

【0034】 將進一步僅以舉例方式參照附圖中圖示之本發明之實施例而進一步描述本發明，在該等附圖中：

【0035】 第 1 圖圖示根據一個實施例之具有資料儲存器之資料處理設備，該資料儲存器具有安全區域及非安全區域；

【0036】 第 2 圖示意地圖示根據一個實施例，可如何將資料處理設備之一組暫存器劃分成調用者暫存器及被調用者暫存器；

【0037】 第 3A 圖及第 3B 圖示意地圖示根據一實施例藉由例外控制電路執行之堆疊操作及非堆疊操作；

【0038】第 4 圖示意地圖示在代碼執行期間對於各種不同情況之例外（在此實例中為中斷）之獲得；

【0039】第 5 圖為根據一個實施例圖示當接收到初始例外且然後接收到進一步例外時保存之狀態的表格；

【0040】第 6 圖圖示對於示例性實施例，取決於為了獲得例外所需之網域轉變之暫存器，該暫存器之狀態在獲得例外時保存至堆疊；

【0041】第 7A 圖及第 7B 圖圖示根據一個實施例之兩個示例性尾鏈情況；

【0042】第 8A 圖及第 8B 圖圖示根據一個實施例之兩個進一步尾鏈情況；

【0043】第 9A 圖及第 9B 圖圖示根據一個實施例之兩個早期搶先情況；

【0044】第 10 圖示意地圖示根據一個實施例當處理搶先例外時可使用之分解技術；

【0045】第 11 圖示意地圖示根據一個實施例儲存包括安全性位元之例外返回值之鏈接暫存器的使用；

【0046】第 12 圖為圖示根據一個實施例，在接收到例外之時執行的堆疊操作之流程圖；及

【0047】第 13 圖為圖示根據一個實施例，在完成例外之時執行的非堆疊操作之流程圖。

【實施方式】

【0048】第 1 圖圖示可例如為微控制器之資料處理設備 10。該資料處理設備 10 包含用於處理指令之處理電路 20 及

用於儲存資料且亦用於儲存程式碼之資料儲存器 30，該資料係由處理電路 20 處理，該程式碼由處理電路 20 執行。

【0049】資料儲存器 30 具有兩個不同安全性之區域，該兩個區域為安全區域 32 及非安全區域 34(在本文中亦稱為較不安全區域)。儲存於安全區域 32 中之資料在執行時對儲存於非安全區域 34 中之代碼不可存取。

【0050】資料處理設備 10 亦具有記憶體保護單元 MPU(memory protection unit; MPU) 40，該記憶體保護單元 MPU 40 控制對安全區域 32 及非安全區域 34 之存取。儘管此控制可經由記憶體保護單元執行，但在其他實施例中，此控制亦可由處理設備之內的電路以更分散式方式進行，該電路監視當前正在執行之儲存之區域碼，且該電路依賴於該區域碼控制對記憶體之不同區域之存取。

【0051】在此實施例中，正在執行處理電路 20 之網域之安全性係根據儲存當前正在執行之代碼的區域決定（用於決定操作之當前網域的其他技術亦是可能的）。因此，儲存於安全資料儲存器 32 中之安全程式碼係執行於安全網域中，且使用安全堆疊 36 以儲存資料值。類似地，儲存於非安全資料儲存器 34 中之非安全代碼係執行於非安全網域（在本文中亦稱為較不安全網域）中，且該非安全代碼在執行期間使用非安全堆疊 38 用於儲存資料值。

【0052】處理電路 20 具有用於提取待執行之指令的提取電路 22。處理電路 20 亦具有用於解碼該等指令之解碼電路 24 及用於執行該等指令之執行電路 26。待執行之指令係由提

取電路 22 經由記憶體保護單元 MPU 40 自資料儲存器 30 提取。該等指令及資料係經由 MPU 40 擷取，該 MPU 40 控制對安全區域及非安全區域之存取且將安全資料與非安全側隔離。

【0053】在此實施例中，存在暫存器組 60，該暫存器組 60 具有在資料處理期間使用之通用暫存器。該等通用暫存器具有程式計數器 PC(program counter; PC)及堆疊指標 SP(stack pointer; SP)，該程式計數器 PC 指示何指令為待執行之下一指令，該堆疊指標 SP 指示當前堆疊框於堆疊中位於何處。在此實施例中，由於在安全側中有一堆疊且在非安全側中亦有一堆疊，所以存在安全堆疊指標 SSP 及非安全堆疊指標 NSP，但是該等指標中僅一個指標對於正在任一時刻執行之程式直接可見。應注意，在一些實施例中，對於每一堆疊可能有複數個堆疊指標，但在任一時刻將僅一個堆疊指標可見。在暫存器組 60 中亦存在用於儲存資料值之通用暫存器，該等資料值正由處理電路 20 處理。在此實施例中，該等值經標記為 R0 至 R12。

【0054】暫存器組 60 亦包含鏈接暫存器 65，該鏈接暫存器 65 可用以當獲得例外或調用函數時儲存返回值。返回值允許系統決定返回為例外返回還是函數返回，且決定當自例外或函數返回時需要何處理。可以使用不同類型之返回值，該等返回值包括例外返回(EXC_RETURN)值，該值指示例外返回且可包括資訊（諸如處理背景處理之網域之安全位準的指示），該指示可使處理器能夠決定如何處理例外返回，例如，

當恢復狀態時存取何堆疊且需要載入多少暫存器。

【0055】第 1 圖亦圖示額外暫存器組 64，該額外暫存器組 64 具有諸如浮點暫存器之額外專用暫存器。在一個實施例中，可在安全配置暫存器(secure configuration register; SCR) 62 中設定值以識別額外暫存器組 64 中之暫存器中之任一暫存器是否能夠儲存安全資料，且若有，則彼等暫存器將被視為形成一組暫存器之一部分(與暫存器組 60 之暫存器一起)，當控制自安全網域至較不安全網域之轉變時需要管理該組暫存器之該部分，且反之亦然。

【0056】根據所描述之實施例，可用於在安全性網域之間轉變的一個機制為例外機制。根據此機制，在發生例外時，當前軟體常式之執行將暫時停止，且取而代之的是，執行將分支至用於處理例外之例外處理常式，所使用之例外處理常式係取決於發生之例外的類型。一旦已執行例外處理常式，然後將使用例外返回以返回至初始軟體常式，該初始軟體常式係由於發生之例外而暫時停止。

【0057】提供例外控制電路 28 以控制例外之獲得，且其中該等例外導致自較安全網域至較不安全網域之轉變，可儲存敏感資料之該組暫存器將在獲得例外之前清空，以避免儲存於該等暫存器中之資料可用於非安全側。儲存於一些或所有該等暫存器中之狀態將在例外控制電路 28 之控制下儲存在安全堆疊上，以使得在自例外返回時，可恢復彼狀態。

【0058】雖然在第 1 圖中，資料儲存器 30 含有單個安全區域及單個非安全區域，但是本文所述之技術皆同樣地適合

於包含多於兩個不同安全性區域之不同實施。

【0059】此外，雖然第 1 圖圖示例外控制電路 28 與處理電路 20 之其他部分（諸如執行平台 26）分離，但是實務上，例外控制電路 28 可至少部分地重新使用處理電路 20 之一些元件以控制例外之處理。

【0060】在第 2 圖中示意地圖示當控制自安全網域至較不安全網域之轉變時需要管理之一組暫存器 100，且反之亦然。根據所描述之實施例，將一些該等暫存器定義為調用者暫存器 110，而將其他暫存器定義為被調用者暫存器 120。調用者暫存器為例外控制電路 28 將總是負責狀態保存至堆疊上之彼等暫存器，而與執行例外處理常式所處之網域無關。在預設情況下，例外處理常式隨後將具有狀態保存被調用者暫存器之責任。特定言之，例外處理常式隨後將保存被調用者暫存器之狀態至與網域相關聯之堆疊上，在該網域中正在執行例外處理常式。進一步地，例外處理常式隨後將負責在發出例外返回之前恢復彼等被調用者暫存器之狀態（典型地藉由將該等被調用者暫存器之狀態自堆疊複製回至相關暫存器中）。

【0061】然而，根據所描述之實施例，在例外將需要自安全網域至較不安全網域之轉變，且背景處理在安全網域中之情況下，例外控制電路 28 另外地負責在引起處理電路轉變以執行例外處理常式之前將被調用者暫存器狀態保存在安全堆疊 36 之堆疊框之內。

【0062】如上所述，SCR 暫存器 62 之內容將定義哪些暫存器可用以儲存安全資料，且因此定義哪些暫存器需要包含

於該組暫存器 100 之內。在一個實施例中，SCR 暫存器 62 之內容將識別是否除通用暫存器 60 之外還有額外專用暫存器 64 中之任一者亦包含於該組 100 之內。

【0063】第 3A 圖圖示對於三個不同情況，在發生例外時且在隨後完成彼例外時之例外控制電路之操作。該等情況中之第一情況為其中背景處理處於安全網域中之情況，且例外係待由安全網域中之例外處理常式處理；該等情況中之第二情況為其中背景處理處於非安全網域中之情況，且例外係待由安全網域中之例外處理常式處理；且第三情況為其中背景處理處於非安全網域中之情況，且例外係待由非安全網域中之例外處理常式處理。

【0064】在該三個情況中之每一情況中，當背景處理 130 係由例外中斷時，例外控制電路 28 經安排以在觸發處理電路執行所需例外處理常式 140 以處理該例外之前，在點 135 處將來自調用者暫存器之資料堆疊至與正在執行背景處理之網域相關聯之堆疊上。在完成執行之時，例外控制電路亦在點 150 處恢復背景處理之前，在點 145 處將來自相關堆疊之先前堆疊之資料解堆疊回至調用者暫存器。

【0065】例外處理常式將通常在例外處理常式期間重新使用該等暫存器之前負責堆疊來自被調用者暫存器之資料，且用於稍後在例外處理常式結束之前將彼資料解堆疊回至被調用者暫存器。

【0066】在第 3A 圖之實例中，取決於特定實施，在執行例外處理常式之前，調用者暫存器可能由或可能不由硬體清

空。在一個實施例中，將不清空調用者暫存器之內容，因為設想之三個情況當獲得例外時不在網域中導致轉變，或僅導致自不安全至安全網域之轉變，且在一個實施例中，允許安全網域看見非安全資料。

【0067】第 3B 圖圖示對於其中背景處理正在安全網域中處理之情況，在發生例外時且在隨後完成彼例外時之例外控制電路之操作，且該例外需要至非安全網域之轉變。在此實施例中，當背景處理 160 由例外中斷時，例外控制電路在點 165 處經配置以將來自調用者暫存器之資料堆疊至安全堆疊上，且另外例外控制電路在點 170 處經安排以將來自被調用者暫存器之資料堆疊至安全堆疊上。例外控制電路隨後亦將確保調用者暫存器及被調用者暫存器之內容在觸發處理電路執行例外處理常式 175 之前得以清空。因此，在此情況中，非安全例外處理常式對先前保持於調用者暫存器或被調用者暫存器中之安全資料不具有存取權限。

【0068】在完成例外處理常式時，在於點 190 處恢復背景處理之前，例外控制電路隨後將在點 180 處將來自安全堆疊之先前堆疊之被調用者資料解堆疊回至被調用者暫存器中，且例外控制電路亦將在點 185 處將來自安全堆疊之先前堆疊之調用者資料解堆疊回至調用者暫存器中。

【0069】在一個特定實施例中，非安全例外處理常式仍可經安排以照常保存被調用者暫存器之狀態，但在此情況中，彼等被調用者暫存器將為空，且因此例外處理常式將僅儲存清空值至非安全堆疊上，該例外處理常式將稍後在發出例外

返回之前恢復該非安全堆疊至暫存器中。

【0070】 如上文所解釋，作為架構中之預設位置，當例外（例如中斷）發生且完成時，部分暫存器狀態係藉由硬體自動地保存且恢復。在中斷引起安全至非安全轉變之情況下，藉由延伸該架構以保存且清空安全網域使用之整體暫存器狀態或至少所有暫存器狀態，硬體能夠維持例外周圍之安全性。

【0071】 藉由使用上述技術，有可能藉由延伸自動暫存器堆疊系統以引起例外控制電路推動所有調用者暫存器及被調用者暫存器至堆疊（而非僅調用者保存暫存器），且然後在切換至非安全狀態且跳躍至例外處理常式（中斷之實例中的中斷向量）之前清空暫存器值來移除經由安全狀態代理中斷之要求。為了保持中斷延遲儘可能低，當自安全狀態轉變至非安全狀態時，僅推動額外暫存器狀態至堆疊上。當較高優先級例外（所謂的搶先例外）在例外處理期間發生時，或當處理尾鏈例外時，此舉引入一些複雜性。第 4 圖圖示一些實例。

【0072】 在第一實例中，在安全狀態中執行背景程式碼且接收第一安全中斷。將一子集之暫存器（亦即，調用者暫存器）保存至安全堆疊，且然後（同時第一安全中斷係仍然經由適當中斷向量處理）接收需要在非安全網域中處理的第二較高優先級中斷。由於該第二較高優先級中斷需要在非安全網域中之處理，所以在安全暫存器中無資訊應對於新中斷向量常式可見，且因此所有安全暫存器（調用者暫存器及被調用者暫存器兩者）皆應保存至安全堆疊且然後在獲得此中斷

之前清空。當第二中斷已完成時，處理返回至未完成初始安全中斷，且回應於第二中斷經推動至安全堆疊之暫存器係藉由彈出安全堆疊在彼點處恢復。然後，此第一安全中斷可完成，此時在繼續安全背景處理之前，推動至堆疊之原始子集可接著藉由彈出安全堆疊而恢復。

【0073】在第二實例中，第二中斷具有比第一中斷低的優先級，且相應地第一中斷將因此在獲得不安全第二中斷之前完成。一旦第一中斷已完成，則推動剩餘暫存器（亦即被調用者暫存器）至安全堆疊，且在獲得非安全中斷之前清空所有暫存器。雖然在此點清空調用者及被調用者暫存器兩者是重要的，但是例外控制電路實際上可能不需要在此階段清空所有暫存器，因為例如調用者暫存器可能早已清空。在非安全中斷結束時，恢復已經推動至安全堆疊之所有暫存器。

【0074】第三實例圖示接收安全中斷之非安全背景代碼，此時存在暫存器（調用者暫存器）至非安全堆疊之部分保存。若然後以較高優先級接收第二非安全中斷，則所有安全暫存器（調用者及被調用者）將需要推動至安全堆疊，且在可獲得安全堆疊之前將該等安全暫存器清空。當非安全中斷完成時，需要自堆疊彈出所有安全暫存器，且隨後當安全中斷完成時，彈出非安全暫存器之原始子集。

【0075】第四實例圖示接收安全中斷之安全背景代碼，該安全中斷引起調用者保存暫存器得以推動至安全堆疊，但是在此程序完成之前，第二較高優先級非安全中斷發生。此第二中斷引起剩餘暫存器（亦即，被調用者暫存器）在已經堆

疊調用者暫存器之後得以推動至安全堆疊上，導致正在執行的所有暫存器的推動。然後，在獲得非安全中斷之前清空所有暫存器。在完成此中斷之後，被調用者保存暫存器在獲得安全中斷之前自安全堆疊彈出。當安全中斷完成時，原始調用者暫存器係自安全堆疊彈出。

【0076】第 5 圖圖示指示潛在中斷及需要執行之狀態保存的表格。就此而言，「推動子集」為將調用者保存子集之暫存器推動至堆疊上，「推動剩餘」為將被調用者保存子集之暫存器推動至堆疊上，且「推動所有」為將調用者暫存器狀態及被調用者暫存器狀態兩者推動至堆疊上。就此而言，在一些暫存器不可用於儲存敏感資料且為已知之情況下，則該等暫存器可能不需要推動至堆疊上。

【0077】在表中，若具有比初始中斷高之優先級的進一步中斷在分支至初始中斷的例外向量（該情況在本文中將稱為早期搶先情況）之前發生，則「例外入口」行識別推動何狀態至堆疊上。若具有比初始中斷低之優先級或與初始中斷之優先級相等之進一步中斷發生，則「例外返回」行識別推動、彈出或清空何狀態，且因此不獲得進一步中斷直至初始中斷完成為止（此舉在本文中將稱為尾鏈情況）。雖然在表中識別之動作通常為由例外控制電路硬體 28 進行之動作，在其中背景處理處於非安全網域中之情況下，清空與安全中斷之後的非安全中斷之尾鏈相關聯的調用者暫存器之動作（「清空子集」）可實際上由軟體而非例外控制電路硬體執行。在其中背景處理處於安全網域中，其中軟體可經安排以清空調用

者暫存器，同時，硬體隨後將推動且清空被調用者暫存器之情況下，此舉對於與安全中斷之後的非安全中斷之尾鏈相關聯的暫存器清空的至少一部分（形成「推動剩餘且清空所有」操作的一部分）之情況亦一樣。

【0078】如自第 5 圖之表的檢視可見，當自安全狀態轉變至非安全狀態時，需要自暫存器移除可保存安全狀態之所有暫存器中之值，以便該等值不可用於非安全側，且因此除通常調用者保存暫存器狀態之外還可執行額外保存及清空。

【0079】第 6 圖圖示一個實施例之堆疊框，且特定言之當自相同或較不安全狀態（第 6 圖之左手側）獲得中斷時保存至堆疊之堆疊框上的暫存器內容，及當轉變至較不安全狀態（第 6 圖之右手側）時保存至堆疊框上之內容。就此而言，由於暫存器無法留下儲存任何狀態且由於此狀態為對於較不安全狀態必須不可用之安全狀態，所以需要在後一情況保存且清空更多暫存器。

【0080】第 6 圖識別根據特定實施例哪些暫存器被視為調用者暫存器且哪些暫存器被視為被調用者暫存器。然而，如上所述，確切來說哪些暫存器需要包括在調用者暫存器及被調用者暫存器之內可取決於實施例而改變，且該等暫存器可藉由安全配置暫存器 62 中之值指示，以使得可藉由使用該值決定所需的狀態保存及暫存器清空。此值可藉由用於特定設備之編譯器設定，且如此允許以不同的方式使用特定設備，且在產品中提供一些靈活性。在其他實施例中，此值可例如當系統啟動時由軟體設定。

【0081】如將自上文所述可知，當例外發生時，例外控制電路將暫存器狀態之調用者保存部分自動地推動且彈出至堆疊，且必要時例外控制電路對使用何堆疊指標且因此使用何堆疊進行改變。如此允許甚至在具有安全網域及較不安全網域之系統中存在以下優點：降低之中斷延遲；減少之中斷抖動；例外處理程式可以 C 語言而非彙編程式寫入；如此允許最佳化，如例外入口及尾鏈上之例外。

【0082】第 7A 圖及第 7B 圖圖示一些特定尾鏈示例性情況。在第 7A 圖之實例中，安全背景處理正在點 250 處執行，但在點 255 處，發生需要例外處理常式待的安全網域中執行之初始例外。因此，在點 255 處，例外控制電路將來自調用者暫存器之資料堆疊至安全堆疊上，然後在點 260 處執行例外處理常式。

【0083】在點 257 處，發生進一步較低優先級之例外，且因此彼例外保持待決直至初始例外在點 265 處完成為止。在此點處，例外控制電路決定需要自安全至非安全網域之轉變以處理進一步例外，且因此在彼點處堆疊被調用者暫存器。亦確保在觸發處理電路以在非安全網域中執行所需例外處理常式以在點 270 處處理進一步例外之前，已將被調用者暫存器清空（調用者暫存器已例如由軟體較早地清空）。在點 275 處完成進一步例外時，例外控制電路然後在於點 280 處繼續背景處理之前解堆疊所有調用者及被調用者暫存器之內容。

【0084】第 7B 圖圖示類似實例，但在此實例中，在點 300 處之背景處理係處於非安全網域中。當初始例外在點 305 處

發生時，在用於初始例外之例外處理常式隨後在點 310 處執行之前，例外控制電路正如例外控制電路在第 7A 圖之實例中所做的一樣堆疊調用者暫存器。然後，將在點 307 處發生之進一步較低優先級之例外保持待決，直至初始例外之處理在點 315 處結束為止。然而，在此點處，因為背景處理不安全，所以例外控制電路不執行堆疊。如上文參照第 5 圖之表格所論述，在此階段可採取之可選步驟為清空調用者暫存器，但此步驟可替代地由軟體而非例外控制電路硬體執行。此後，進一步例外之例外處理常式係在點 320 處在非安全網域中處理。在於點 325 處完成進一步例外時，例外控制電路在於點 330 處返回至背景處理之前解堆疊調用者暫存器。

【0085】 在一個實施例中，第 7A 圖之實例僅為其中當將進一步例外處理為完成初始例外之後的尾鏈例外時例外控制電路必須執行一些額外堆疊的實例，且因此將執行堆疊之額外負擔保持最少，同時當處理尾鏈例外時，保持安全資料之安全性。

【0086】 第 8A 圖及第 8B 圖圖示兩個進一步尾鏈實例。在第 8A 圖之實例中，安全背景處理係正在點 350 處執行，但在點 355 處，發生需要在非安全網域中執行例外處理常式之初始例外。因此，在點 355 處，例外控制電路將來自調用者暫存器及被調用者暫存器之資料堆疊至安全堆疊上，然後在點 360 處執行例外處理常式。

【0087】 在點 357 處，發生進一步較低優先級之例外，且因此彼例外保持待決直至初始例外在點 365 處完成為止。在

此點處，例外控制電路決定需要自非安全網域至安全網域之轉變以處理進一步例外，且因此在觸發處理電路以在安全網域中執行所需例外處理常式以在點 370 處處理進一步例外之前，例外控制電路在彼點處解堆疊被調用者暫存器。在於點 375 處完成進一步例外時，例外控制電路然後在於點 380 處繼續背景處理之前解堆疊調用者暫存器之內容。

【0088】第 8B 圖圖示類似實例，但在此實例中，在點 400 處之背景處理係處於非安全網域中。當在點 405 處發生初始例外時，在初始例外之例外處理常式然後於點 410 處執行之前，例外控制電路堆疊調用者暫存器。然後，將在點 407 處發生之進一步較低優先級之例外保持待決，直至初始例外之處理在點 415 處結束為止。然而，在此點處，例外控制電路決定不需要堆疊操作。此後，進一步例外之例外處理常式係在點 420 處之安全網域中處理。在於點 425 處完成進一步例外時，例外控制電路在於點 430 處返回至背景處理之前解堆疊調用者暫存器。

【0089】在一個實施例中，第 8A 圖之實例僅為其中當將進一步例外處理為完成初始例外之後的尾鏈例外時例外控制電路必須執行解堆疊操作的簡單尾鏈情況中之實例，且因此將執行解堆疊之額外負擔保持最少，同時當處理尾鏈例外時，保持安全資料之安全性。

【0090】第 9A 圖及第 9B 圖圖示根據一個實施例之兩個早期搶先情況。在第 9A 圖之實例中，在安全網域中於點 450 處執行之背景處理具有優先級位準 1，但是在接收到具有優先

級位準 10 且需要安全網域中之處理的例外時，例外控制電路開始在點 455 處堆疊調用者暫存器以爲在點 460 處至安全例外處理常式之轉變作準備。然而，在完成調用者暫存器之堆疊之前，在點 465 處接收進一步例外，該進一步例外具有較高優先級位準（在此實例中爲優先級位準 12），且需要至非安全網域之轉變。如第 9A 圖之右手側上所示，在此點處，修改例外控制電路之堆疊活動，以使得該例外控制電路堆疊調用者暫存器及被調用者暫存器（見點 470）兩者，然後觸發處理電路以在點 475 處於非安全網域中執行進一步例外之例外處理代碼。此後，可接著將優先級位準 10 之安全例外處理爲尾鏈例外。

【0091】 在第 9B 圖之實例中，在安全網域中於點 500 處執行之背景處理具有優先級位準 1，但是在接收到具有優先級位準 10 且需要非安全網域中之處理的例外時，例外控制電路開始在點 505 處堆疊調用者暫存器及被調用者暫存器以爲在點 510 處至非安全例外處理常式之轉變作準備。然而，在完成暫存器之堆疊之前，在點 515 處接收進一步例外，該進一步例外具有較高優先級位準（在此實例中爲優先級位準 12），且需要至安全網域之轉變。如在第 9B 圖之右手側上所示，此點處，例外控制電路之堆疊活動經修改以使得該例外控制電路僅堆疊調用者暫存器（見點 520），且若有必要，此舉涉及將已發生之任何被調用者暫存器堆疊之效應反向（例如藉由將彼等受影響之被調用者暫存器之資料解堆疊）。此後，觸發處理電路以在點 525 處於安全網域中執行進一步例外之例

外處理代碼。此後，可接著將優先級位準 10 之安全例外處理為尾鏈例外。

【0092】第 10 圖示意地圖示根據一個實施例，當處理搶先例外時可使用之分解技術。不同於參看第 9A 圖及第 9B 圖所論述之較早實例，在第 10 圖之實例中假定，在搶先例外發生時，與當前例外相關聯之任何狀態保存已發生，且已觸發處理電路執行必要的例外處理常式。因此，在此點處，接著將需要中斷當前例外處理常式之處理以允許搶先例外得以獲得。

【0093】如第 10 圖中所示，在該等情況中，搶先例外之各種階層可藉由改變將何視為背景處理而分解。特定言之，如由轉變 550、轉變 560 所示，該等轉變 550、560 可分解回至簡單情況 565，且因此當獲得第一例外時，背景處理為安全處理 S_1 ，且最終當完成第一例外時，返回至之背景處理再次為 S_1 。對於第二例外，在獲得搶先例外時，將背景處理之視圖改變（如由虛線圓 555 示意地圖示），以使得將背景處理視為非安全處理 N_2 ，且由此例外控制電路將彼搶先例外作為簡單情況 570 處理。因此，為了決定當獲得例外 S_3 時需要何狀態保存及/或恢復，例外控制電路會將背景處理作為非安全處理 N_2 來處理。

【0094】如第 11 圖中所示，在一個實施例中，為了例外控制電路能夠決定何堆疊自例外返回之何時恢復暫存器狀態，且處理電路應返回至何網域，鏈接暫存器 590 可經設定至特殊 EXC_RETURN 值，而非返回位址。該 EXC_RETURN

值可包括安全性位元，該安全性位元向處理設備指示當背景處理在獲得例外之前執行時，處理電路所在的網域之安全位準。要返回至之實際程式計數器位置與其他暫存器狀態一起儲存於該網域之堆疊上。在此情況下，分支至 EXC_RETURN 值指示返回位址係在堆疊上且該堆疊為何堆疊。

【0095】在一個實施例中，鏈接暫存器 590 不必在例外處理常式正在執行之全部時間中保持 EXC_RETURN 值，且取而代之的是，鏈接暫存器 590 可在開始時設定至此值，且然後鏈接暫存器 590 在不久後移動至堆疊。當例外完成時，軟體分支至由 EXC_RETURN 值指示之位址，CPU 將該值認為是特殊事件，因為該值不為有效指令位址。

【0096】若獲得搶先例外，則在鏈接暫存器中為新搶先例外設定新 EXC_RETURN 值之前（其中安全性位元 S 適當地考慮處理被中斷之當前例外之網域設定），當前例外之 EXC_RETURN 值可儲存在相關堆疊上（根據上文論述之過程）。

【0097】第 12 圖為圖示根據一個實施例在接收到例外之時執行的堆疊操作。在步驟 600 處，決定是否已接收到例外，且若已接收到例外，則程序進行至步驟 605，在步驟 605 處決定處理電路當前是否正在執行背景處理，且因此決定此例外是否將為來自背景處理之初始例外。若決定此例外為來自背景處理之初始例外，則程序進行至步驟 610，在步驟 610 處，決定當獲得例外時是否將需要安全至非安全之轉變（亦即，背景處理是否處於安全網域中，且所需例外處理常式是否將

需要在非安全網域中執行)。若是如此情況，則在步驟 615 處，調用者暫存器及被調用者暫存器兩者將使該兩者之資料由例外控制電路 28 保存至安全堆疊。若非如此情況，則僅調用者暫存器將該等調用者暫存器之資料在步驟 620 處由例外控制電路堆疊，此資料經保存至何堆疊係由正執行背景處理之網域決定。然後，程序返回至步驟 600。

【0098】若在步驟 605 處，決定在步驟 600 處接收之例外並非來自背景處理之初始例外，則程序進行至步驟 625，在步驟 625 處，決定在步驟 600 處接收之此新的例外是否具有比當前正在處理之現有例外高之優先級。若否，則新的例外將被作為尾鏈例外處理，且在步驟 630 處，將決定是否當前例外已完成。一旦當前例外已完成，則在步驟 635 決定在 EXC_RETURN 值之內是否設定 S 位元 595。若否，則程序進行至步驟 640，在步驟 640 處不執行進一步堆疊，且程序然後返回至步驟 600。

【0099】然而，若設定了 S 位元，指示當獲得來自背景處理之初始例外時處理電路係操作於安全網域中，則在步驟 645 處決定新的例外是否需要安全至非安全轉變以執行所需例外處理常式。若否，則在步驟 640 處再次不執行進一步堆疊，且程序返回至步驟 600。然而，若將需要安全至非安全轉變，則程序進行至步驟 650，在步驟 650 處，在程序隨後返回至步驟 600 之前，在被調用者暫存器之內的資料亦在安全堆疊之內堆疊。

【0100】若在步驟 625 處，決定新的例外確實具有比當前

例外高的優先級，則將新的例外作為搶先例外處理。在步驟 655 處，然後將決定是否仍然對當前例外執行堆疊。若是，則在步驟 660 處，取決於新的例外修改堆疊行為，如先前參看第 9A 圖及第 9B 圖所論述。此後，程序返回至步驟 600。

【0101】若在步驟 655 處，決定堆疊仍未對於當前例外執行，且取而代之的是處理電路已開始執行彼當前例外之相關例外處理常式，則程序進行至步驟 665，在步驟 665 處，將當前例外作為背景處理來處理，且程序隨後返回至步驟 610。因此，在步驟 665 處，執行較早參看第 10 圖論述之分解技術。

【0102】第 13 圖為圖示根據一個實施例，在完成例外之時執行的解堆疊操作之流程圖。在步驟 700 處，決定是否已完成例外，且若已完成例外，則程序進行至步驟 705，在步驟 705 處決定背景處理是否處於安全網域中。如上所述，此舉可參考儲存在 EXC_RETURN 值之內的 S 位元 595 決定。如上所述，若返回之例外為搶先例外，則將背景處理視為由搶先例外中斷之例外處理常式。

【0103】若背景處理是在安全網域中，則在步驟 710 處，決定由於當前例外之完成是否需要非安全至安全之轉變。若是，則在步驟 715 處，解堆疊被調用者暫存器之內容，然後程序進行至步驟 720。若在步驟 710 處，決定不需要非安全至安全之轉變，則程序直接進行至步驟 720。

【0104】在步驟 720 處，決定是否需要由於例外完成返回至背景處理，且若否，則程序返回至步驟 700 以等待完成下一例外。然而，若在步驟 720 處決定需要返回至背景處理，

則程序進行至步驟 725，在步驟 725 處，在程序返回至步驟 700 之前，解堆疊調用者暫存器之內容。

【0105】上述實施例之技術使當回應於例外執行狀態保存時能夠在安全性與效能之間達成改良之平衡，其中例外控制電路之硬體機制使在不需經由例外處理程式代理之情況下能夠有效處理安全例外。

【0106】本申請案之標的係關於在共同讓渡的同在申請中之美國申請案第 13/368,419 號及英國專利申請案第 1217531.1 號中論述之標的，且該等文件兩者之整個內容在此以引用之方式併入。

【0107】雖然已在本文中描述特定實施例，但是應將瞭解，本發明並不限於該等實施例且可在本發明之範疇內對該等實施例進行許多修改及添加。例如，可在不背離本發明之範疇之情況下對獨立項之特徵進行以下附屬項之特徵的各種組合。

【符號說明】

【0108】

- 10 資料處理設備
- 20 處理電路
- 22 提取電路
- 24 解碼電路
- 26 執行電路
- 28 例外控制電路
- 30 資料儲存器

32	安全區域
34	非安全區域
36	安全堆疊
38	非安全堆疊
40	記憶體保護單元
60	暫存器組
62	安全配置暫存器
64	額外暫存器組
65	鏈接暫存器
100	一組暫存器
110	調用者暫存器
120	被調用者暫存器
130	背景處理
135	點
140	例外處理常式
145	點
150	點
160	背景處理
165	點
170	點
175	例外處理常式
180	點
185	點
190	點

250 點
255 點
257 點
260 點
265 點
270 點
275 點
280 點
300 點
305 點
307 點
310 點
315 點
320 點
325 點
330 點
350 點
355 點
357 點
360 點
365 點
370 點
375 點
380 點

400 點

405 點

407 點

410 點

415 點

420 點

425 點

430 點

450 點

455 點

460 點

465 點

470 點

475 點

500 點

505 點

510 點

515 點

520 點

525 點

550 轉變

555 虛線圓

560 轉變

565 簡單情況

570 簡單情況
590 鏈接暫存器
595 S 位元
600 步驟
605 步驟
610 步驟
615 步驟
620 步驟
625 步驟
630 步驟
635 步驟
640 步驟
645 步驟
650 步驟
655 步驟
660 步驟
665 步驟
700 步驟
705 步驟
710 步驟
715 步驟
720 步驟
725 步驟
R0 值

R12 值

【生物材料寄存】

國內寄存資訊【請依寄存機構、日期、號碼順序註記】

無

國外寄存資訊【請依寄存國家、機構、日期、號碼順序註記】

無

【序列表】(請換頁單獨記載)

無

申請專利範圍

1. 一種資料處理設備，該資料處理設備包含：

處理電路，該處理電路經配置以回應於程式碼執行資料處理操作，該處理電路包含用於控制例外處理之例外控制電路；

一資料儲存器，該資料儲存器經配置以儲存資料，該資料儲存器包含複數個區域，該複數個區域包括一安全區域及一較不安全區域，其中該安全區域係用於儲存當操作於一安全網域中時該處理電路可存取且當操作於一較不安全網域中時該處理電路不可存取之資料；以及

複數個暫存器，該複數個暫存器經配置以儲存資料，該等暫存器包括一第一子集之暫存器及一第二子集之暫存器，該等暫存器可存取在該處理電路上執行的該程式碼，其中，回應於一例外，要求進行來自該等暫存器至該資料儲存器之資料的狀態保存，以在該例外被處理時允許該資料稍後至該等暫存器之恢復；

其中：

回應於來自由該處理電路執行之背景處理之一初始例外，該例外控制電路經配置以在觸發該處理電路執行對應於該例外之一例外處理常式之前執行來自該第一子集之暫存器至該資料儲存器之資料的狀態保存，其中該例外處理常式具有執行來自該第二子集之暫存器至該資料儲存器之資料的狀態保存的責任；以及

回應於引起自該安全網域至該較不安全網域之一轉

變的一第一例外，其中該背景處理係藉由該處理電路在該安全網域中執行，該例外控制電路經配置以在觸發該處理電路執行在該較不安全網域中之該例外處理常式之前，執行來自該第二子集之暫存器至該資料儲存器之該資料的額外狀態保存。

2. 如請求項 1 所述之資料處理設備，其中回應於該第一例外，該例外控制電路經配置以在觸發該處理電路執行該例外處理常式之前清空該第二子集之暫存器。
3. 如請求項 2 所述之資料處理設備，其中回應於該第一例外，該資料處理設備經配置以在該例外控制電路觸發該處理電路執行該例外處理常式之前，確保該第一子集之暫存器不含有安全資料。
4. 如請求項 1 所述之資料處理設備，其中若該例外控制電路在觸發該處理電路執行該例外處理常式之前已執行該額外狀態保存，則該例外處理常式不執行該第二子集之暫存器之該狀態保存。
5. 如請求項 1 所述之資料處理設備，其中若該例外控制電路在觸發該處理電路執行該例外處理常式之前已執行該額外狀態保存，則該例外處理常式亦執行該第二子集之暫存器之狀態保存。

6. 如請求項 1 所述之資料處理設備，其中該第一例外包含在該背景處理期間發生之該初始例外。
7. 如請求項 1 所述之資料處理設備，其中該第一例外包含一尾鏈例外，在已處理該初始例外之後且在返回至該背景處理之前處理該尾鏈例外，該背景處理係在該初始例外之前執行。
8. 如請求項 1 所述之資料處理設備，其中回應於當已處理該初始例外時且在該處理電路已返回至該背景處理之前待決之一進一步例外，該背景處理係在該初始例外之前執行，該例外控制電路經配置以在引起該處理電路返回至該背景處理之前將該進一步例外之處理作為一尾鏈例外來控制。
9. 如請求項 1 所述之資料處理設備，其中：

該例外控制電路經配置以回應於具有比一當前例外低之優先級的一新的例外，該當前例外之相應例外處理常式仍正在執行，在引起該處理電路返回至該背景處理之前將該新的例外之處理作為一尾鏈例外來控制；

該例外控制電路經配置以當控制該新的例外之處理時不執行進一步狀態保存操作，除非出現下列情況之一：該當前例外在該安全網域中執行，該新的例外指示切換至該較不安

全網域，及該背景處理係在該安全網域中執行；此時在完成該當前例外之該例外處理常式之後，該例外控制電路經配置以執行來自該第二子集之暫存器之該資料的該額外狀態保存，且確保在觸發該處理電路執行對應於該新的例外之該例外處理常式之前清空該第二子集之暫存器。

10. 如請求項 1 所述之資料處理設備，其中：

該例外控制電路經配置以回應於具有比一當前例外低之優先級的一新的例外，該當前例外之相應例外處理常式仍正在執行，在引起該處理電路返回至該背景處理之前將該新的例外之處理作為一尾鏈例外來控制；

該例外控制電路經配置以當控制該新的例外之處理時不執行狀態恢復操作，除非出現下列情況之一：該當前例外在該較不安全網域中執行，該新的例外指示切換至該安全網域，及該背景處理係在該安全網域中執行；此時在完成該當前例外之該例外處理常式之後，該例外控制電路經配置以在觸發該處理電路執行對應於該新的例外之該例外處理常式之前執行該資料之一狀態恢復操作至該第二子集之暫存器中。

11. 如請求項 1 所述之資料處理設備，其中若在執行該第二

子集之暫存器之該額外狀態保存時發生具有比該第一例外高之一優先級的一搶先例外，且該搶先例外不需要自該安全網域至該較不安全網域之一轉變，則該例外控制電路經配置以在觸發該處理電路處理該搶先例外之該例

外處理常式之前將該額外狀態保存反向。

12. 如請求項 1 所述之資料處理設備，其中若一當前例外不引起自該安全網域至該較不安全網域之一轉變，且若在與該當前例外相關聯之該例外處理常式的處理開始之前發生一搶先例外，該搶先例外具有比該當前例外高之一優先級且需要自該安全網域至該較不安全網域之一轉變，則該例外控制電路經配置以在觸發該處理電路處理該搶先例外之該例外處理常式之前另外地執行來自該第二子集之暫存器的該資料之該額外狀態保存。
13. 如請求項 1 所述之資料處理設備，其中若在該例外控制電路已觸發該處理電路執行對應於一當前例外之該例外處理常式之後，但在彼例外處理常式已完成之前發生一搶先例外，則該例外控制電路經配置以當決定在觸發該處理電路執行該搶先例外之該例外處理常式之前，是否需要該第一子集之暫存器之該狀態保存，或該第一子集之暫存器及該第二子集之暫存器之該狀態保存時，將該當前例外作為該背景處理來處理。
14. 如請求項 1 所述之資料處理設備，其中該資料儲存器包含複數個堆疊，該複數個堆疊包括在該安全區域中之一安全堆疊，及在該較不安全區域中之一較不安全堆疊。

15. 如請求項 14 所述之資料處理設備，其中在來自該第一子集之暫存器的資料之該狀態保存及來自該第二子集之暫存器的資料之該額外狀態保存中，該例外控制電路經配置以將該資料保存至該安全堆疊及該較不安全堆疊中之一者，該安全堆疊及該較不安全堆疊中之一者對應於該網域之安全性，當執行該背景處理時該處理電路在該網域中操作。
16. 如請求項 1 所述之資料處理設備，該資料處理設備進一步包含用於儲存一安全配置值之一安全配置儲存位置，該安全配置值指示該複數個暫存器中之哪些暫存器係可藉由當前執行之代碼用於儲存安全資料，其中回應於引起自該安全網域至該較不安全網域之該轉變的一例外，該例外控制電路經配置以在該第二子集之暫存器之內包括由該安全配置值指示之該等暫存器中之一或更多個暫存器。
17. 如請求項 1 所述之資料處理設備，該資料處理設備進一步包含用於儲存一例外返回值之一儲存位置，該處理電路經配置以在該例外返回值之內設定一網域值，以指示該資料處理設備在自該背景處理獲得一初始例外時操作於其中之網域，該例外控制電路依賴於該網域值決定該等暫存器中之哪些暫存器應經進行狀態保存操作或狀態恢復操作。

18. 一種在一資料處理設備上處理資料之方法，該資料處理設備包含：處理電路，該處理電路用於回應於程式碼執行資料處理操作，該處理電路包含用於控制例外處理之例外控制電路，用於儲存資料之一資料儲存器，該資料儲存器包含複數個區域，該複數個區域包括一安全區域及一較不安全區域，其中該安全區域係用於儲存當操作於一安全網域中時該處理電路可存取，且當操作於一較不安全網域中時該處理電路不可存取之資料，及複數個暫存器，該複數個暫存器經配置以儲存資料，該等暫存器包括一第一子集之暫存器及一第二子集之暫存器，該等暫存器可存取在該處理電路上執行的該程式碼，且其中回應於一例外，要求資料進行來自該等暫存器至該資料儲存器之狀態保存，以在該例外被處理時允許該資料稍後至該等暫存器之恢復；

該方法包含以下步驟：

回應於來自由該處理電路執行之背景處理的一初始例外，使用該例外控制電路以在觸發該處理電路執行對應於該例外之一例外處理常式之前執行來自該第一子集之暫存器至該資料儲存器的資料之狀態保存，其中該例外處理常式具有執行來自該第二子集之暫存器至該資料儲存器之資料的狀態保存之責任；以及

回應於引起自該安全網域至該較不安全網域之一轉變的一第一例外，其中該背景處理係藉由該處理電路在

該安全網域中執行，使用該例外控制電路以在觸發該處理電路執行在該較不安全網域中之該例外處理常式之前執行來自該第二子集之暫存器至該資料儲存器之該資料的額外狀態保存。

19. 一種資料處理設備，該資料處理設備包含：

用於回應於程式碼執行資料處理操作的處理手段，該處理手段包含用於控制例外處理之例外控制手段；

用於儲存資料之資料儲存器手段，該資料儲存器手段包含複數個區域，該複數個區域包括一安全區域及一較不安全區域，其中該安全區域係用於儲存當操作於一安全網域中時該處理手段可存取，且當操作於一較不安全網域中時該處理手段不可存取之資料；以及

複數個暫存器手段，該複數個暫存器手段經配置以儲存資料，該等暫存器手段包括一第一子集之暫存器手段及一第二子集之暫存器手段，該等暫存器手段可存取在該處理手段上執行的該程式碼，其中，回應於一例外，要求進行來自該等暫存器手段至該資料儲存器手段之資料的狀態保存，以在該例外被處理時允許該資料稍後至該等暫存器手段之恢復；

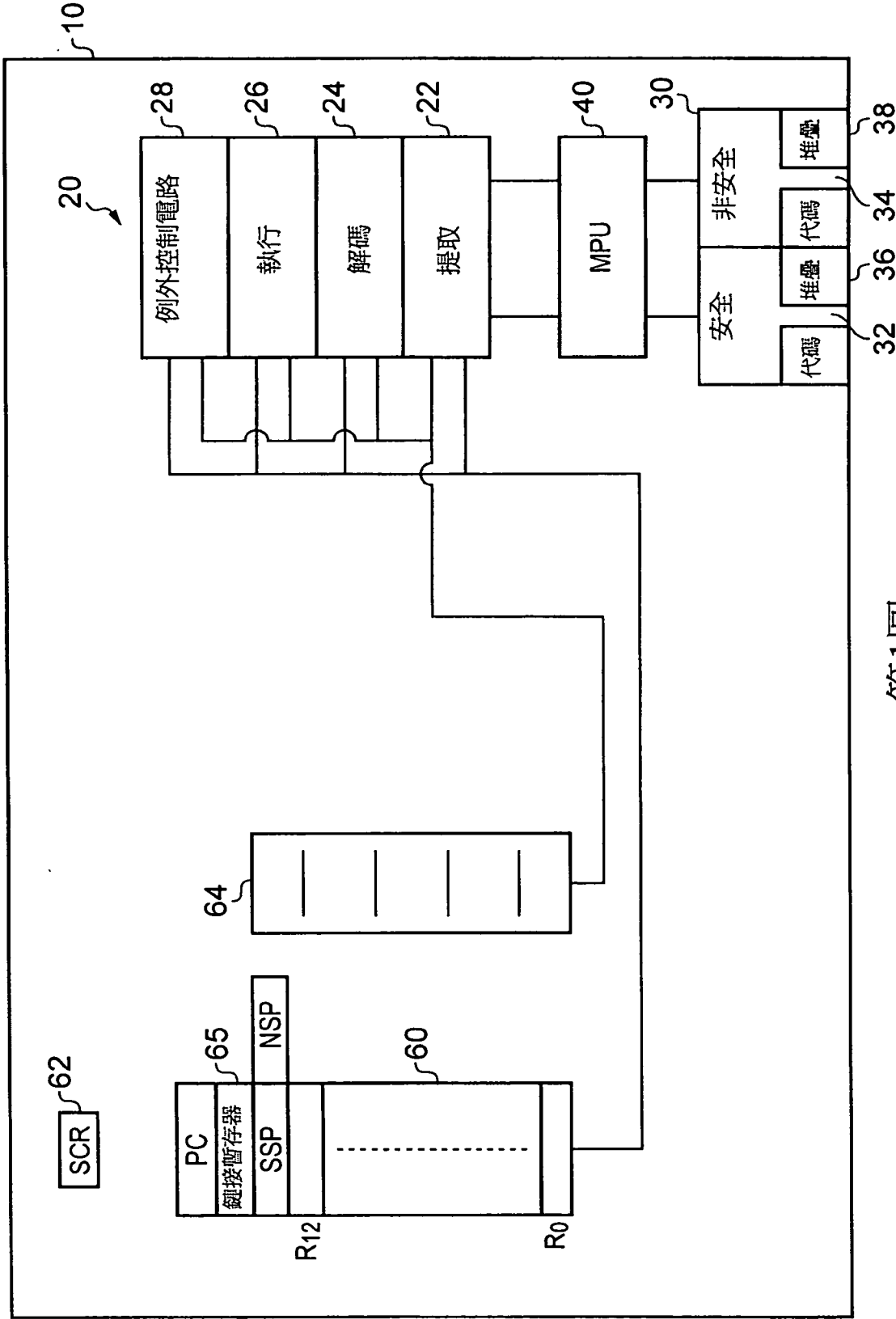
其中：

回應於來自由該處理手段執行之背景處理的一初始例外，該例外控制手段在觸發該處理手段執行對應於該例外之一例外處理常式之前執行來自該第一子集之暫存器

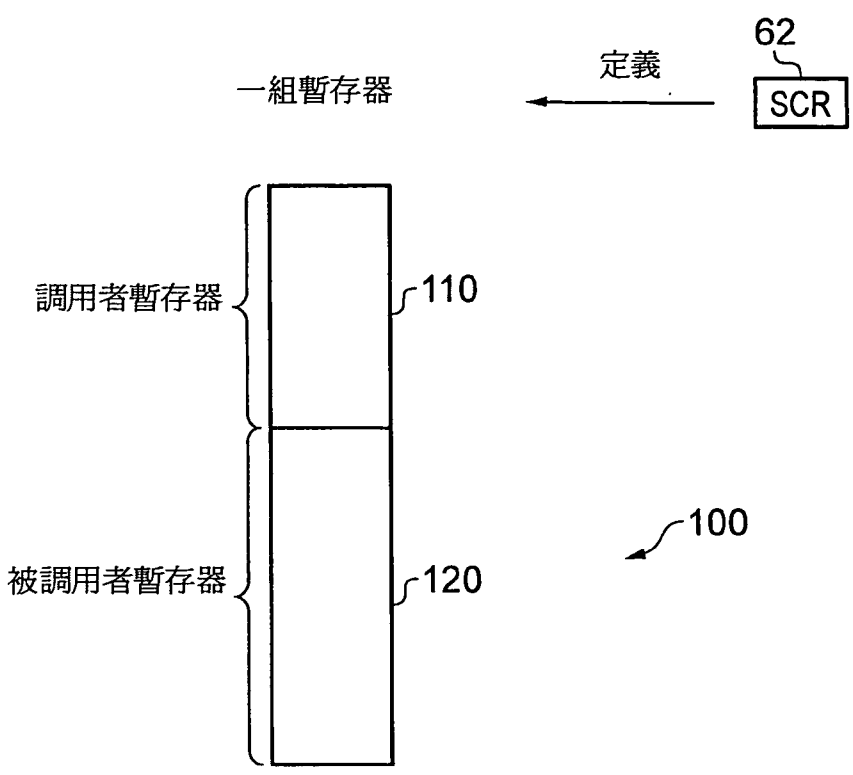
手段至該資料儲存器手段的資料之狀態保存，其中該例外處理常式具有執行來自該第二子集之暫存器手段至該資料儲存器手段之資料的狀態保存之責任；以及

回應於引起自該安全網域至該較不安全網域之一轉變的第一例外，其中該背景處理係藉由該處理手段在該安全網域中執行，該例外控制手段在觸發該處理手段執行在該較不安全網域中之該例外處理常式之前執行來自該第二子集之暫存器手段至該資料儲存器手段之該資料的額外狀態保存。

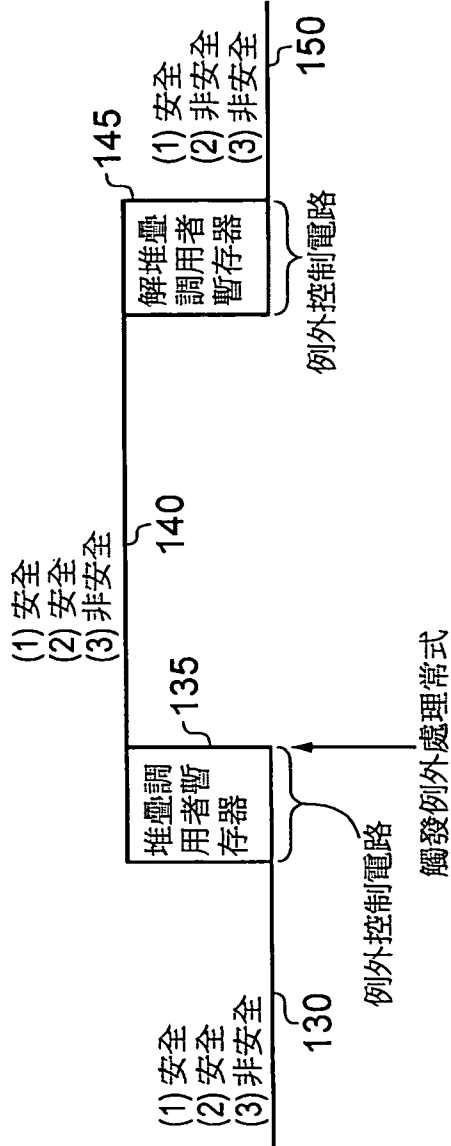
102 年 5 月 23 日修正本



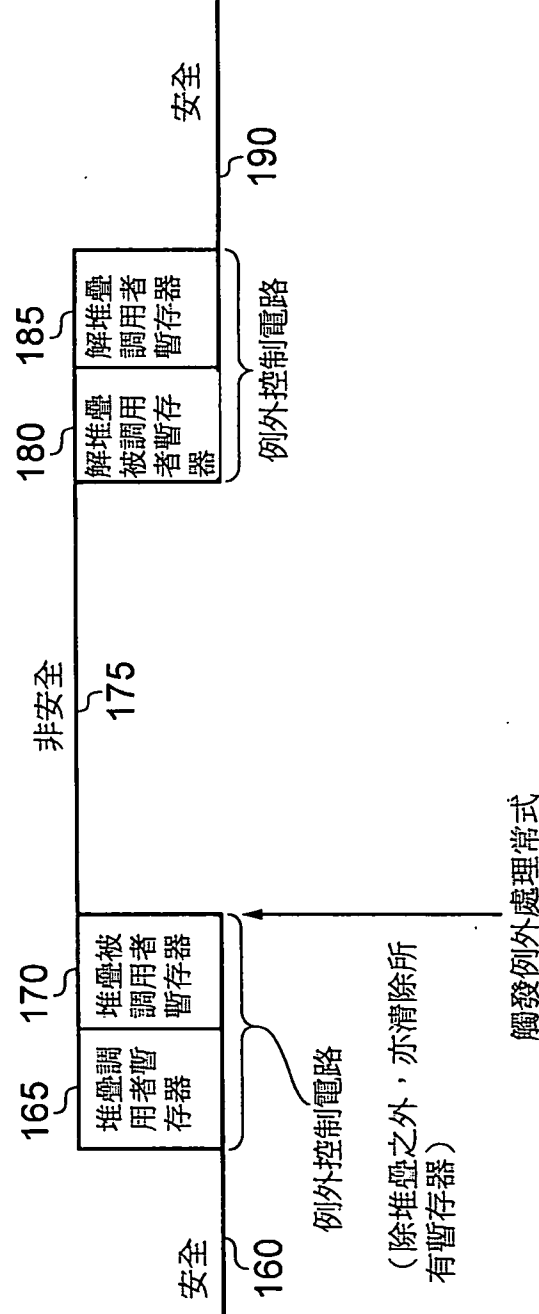
第1圖



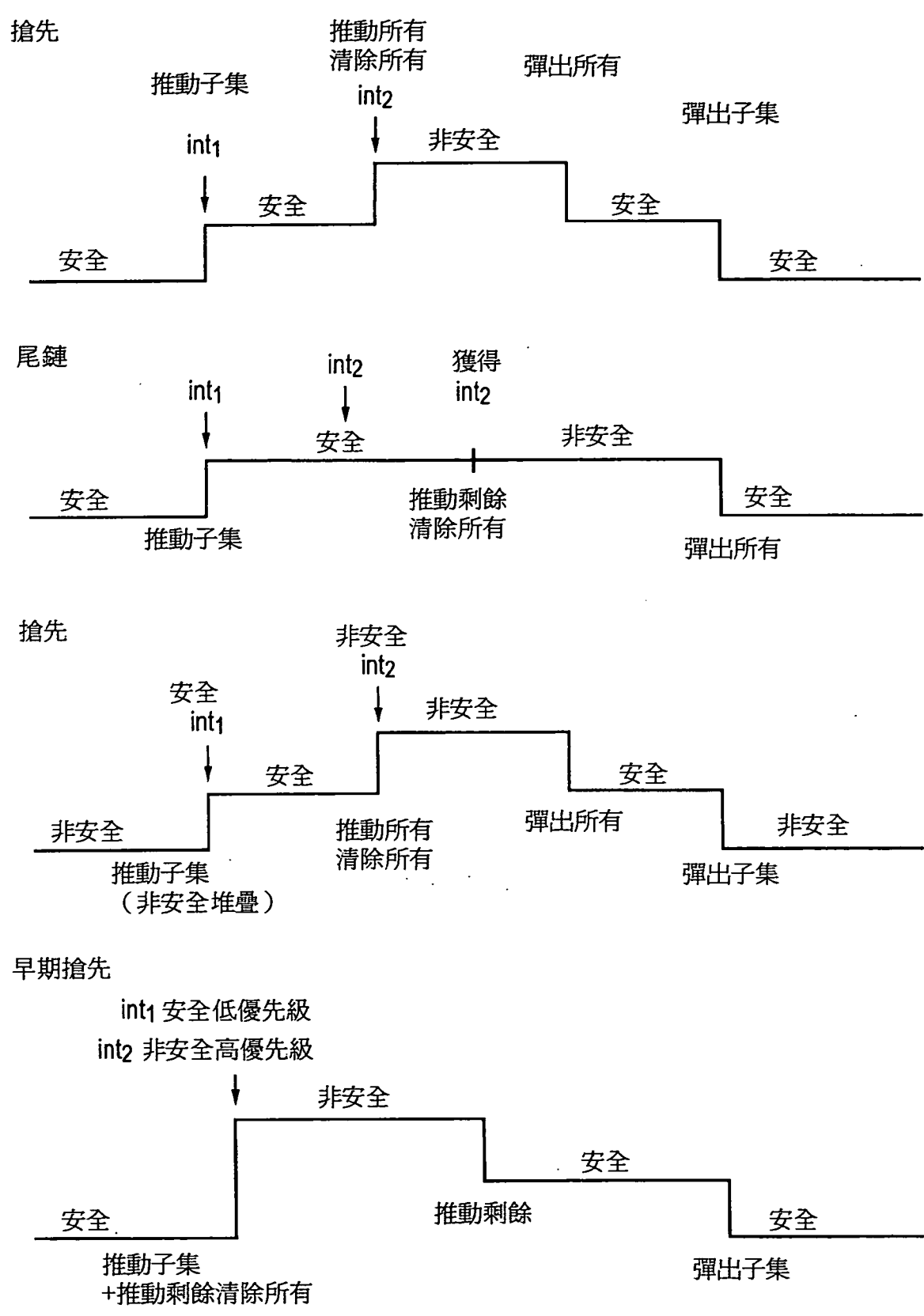
第2圖



第3A圖



第3B圖



第4圖

早期搶先

↓

尾鏈

↓

原始狀態	例外狀態		當第二例外在以下期間發生時待執行之堆疊操作：	
	初始	進一步	例外入口	例外返回
安全	安全	安全	推動子集	無
		非安全	推動且清除所有	推動剩餘且清除所有
	非安全	安全	推動子集	彈出剩餘
		非安全	推動且清除所有	無
非安全	安全	安全	推動子集	無
		非安全	推動子集	清除子集
	非安全	安全	推動子集	無
		非安全	推動子集	無

關鍵：

子集

調用者保存之暫存器狀態之子集

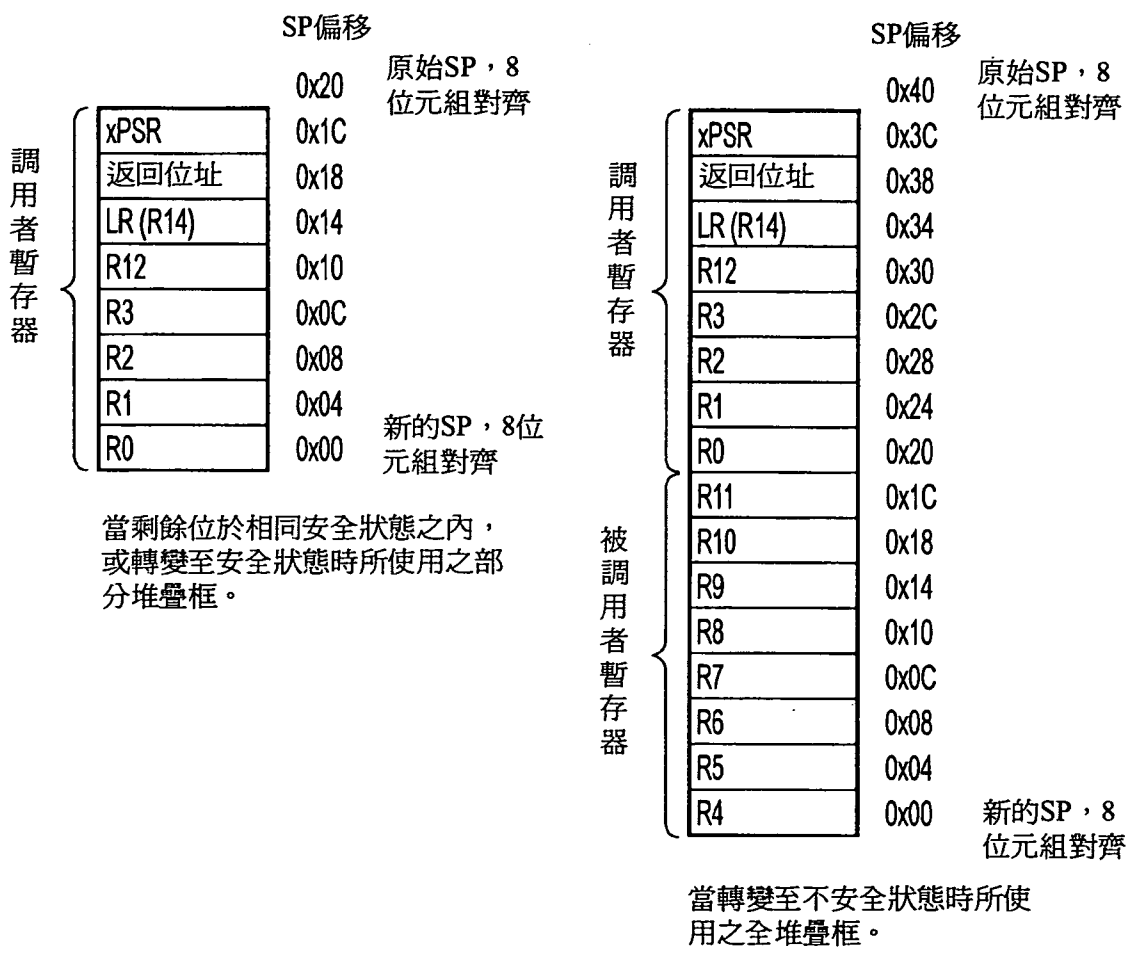
所有

子集及剩餘

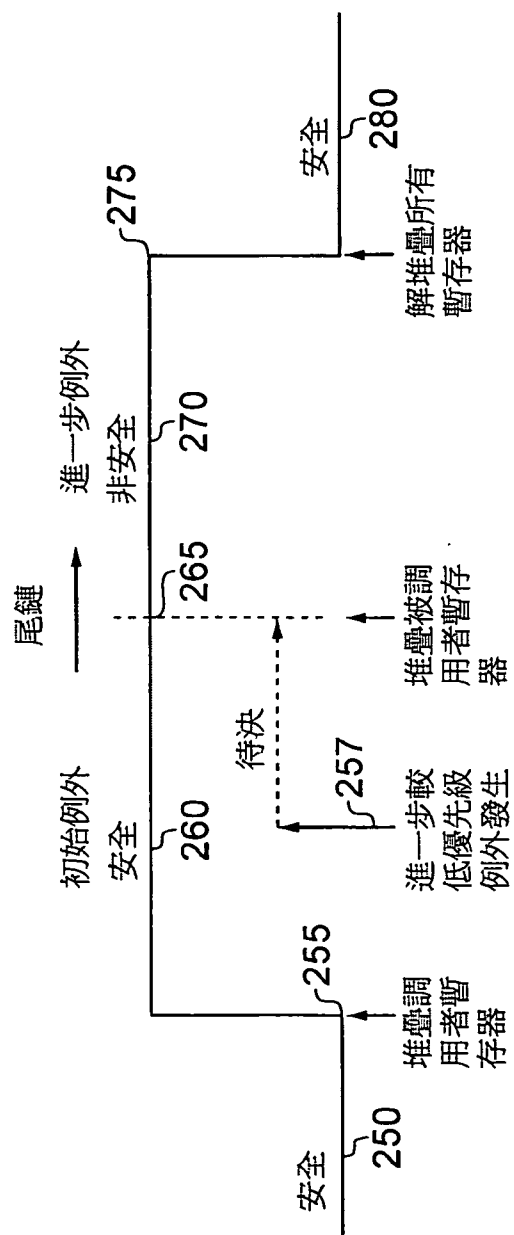
剩餘

被調用者保存之暫存器狀態之子集

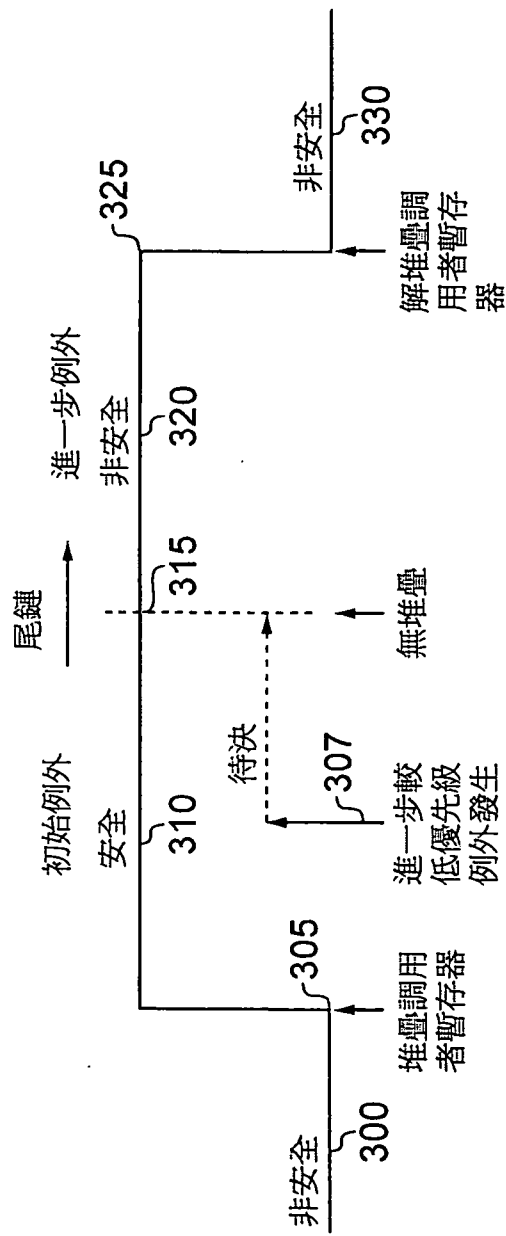
第5圖



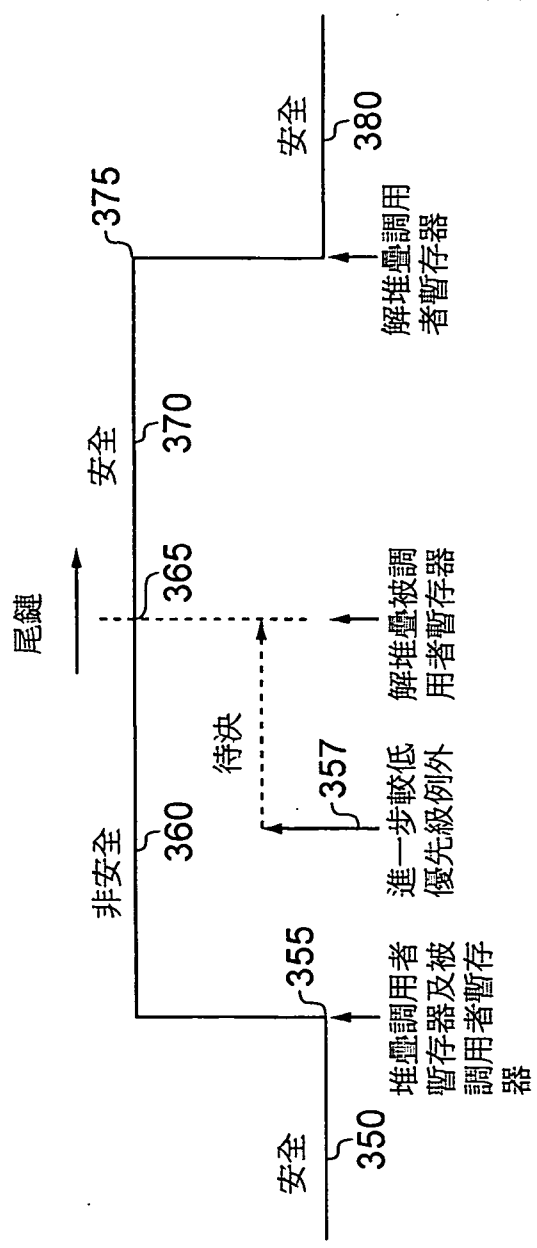
第6圖



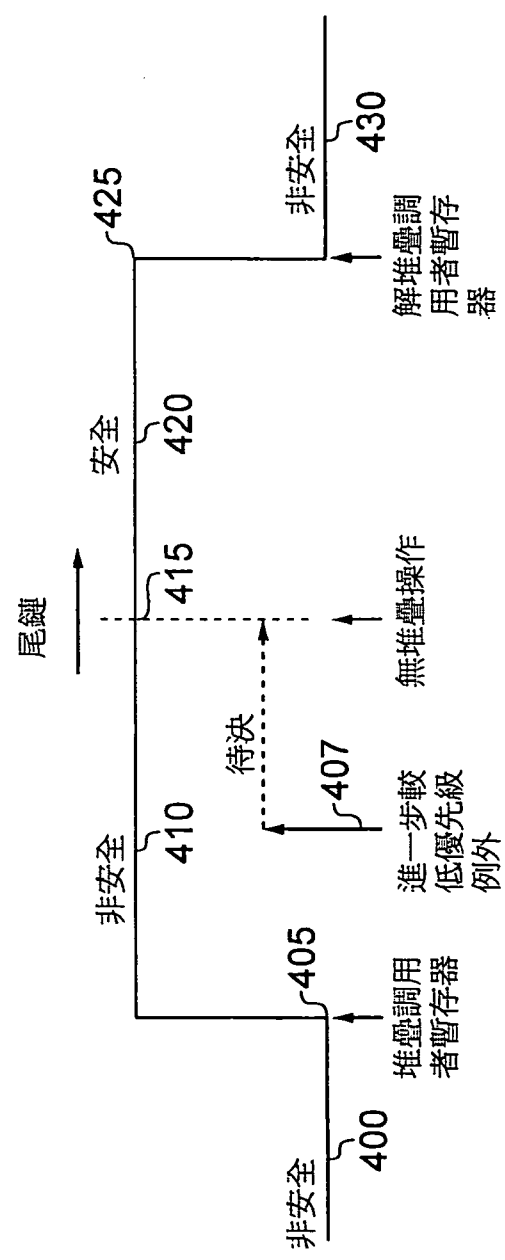
第7A圖



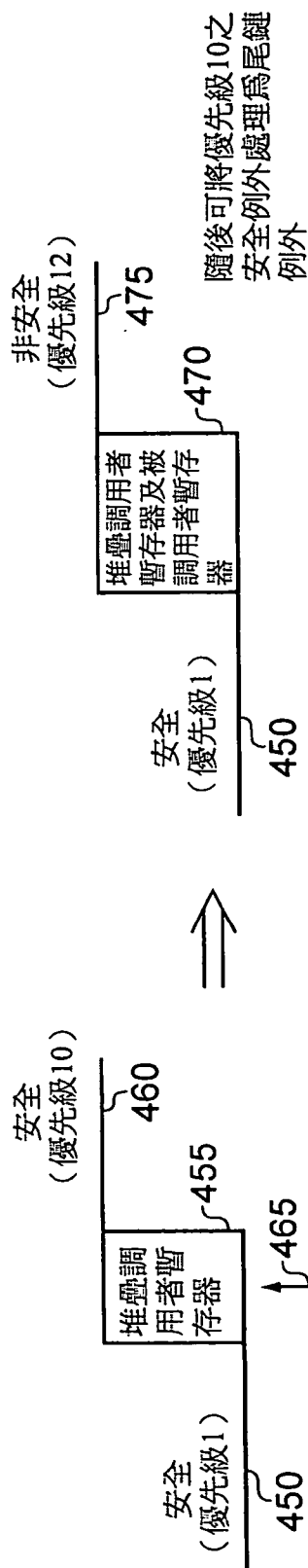
第7B圖



第8A圖



第8B圖



第9A圖

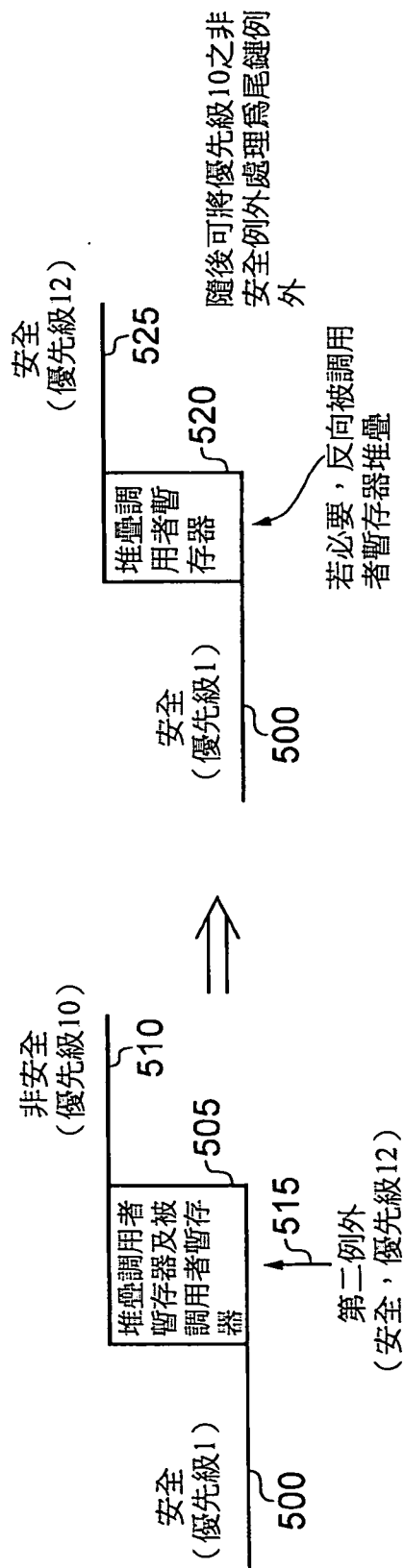
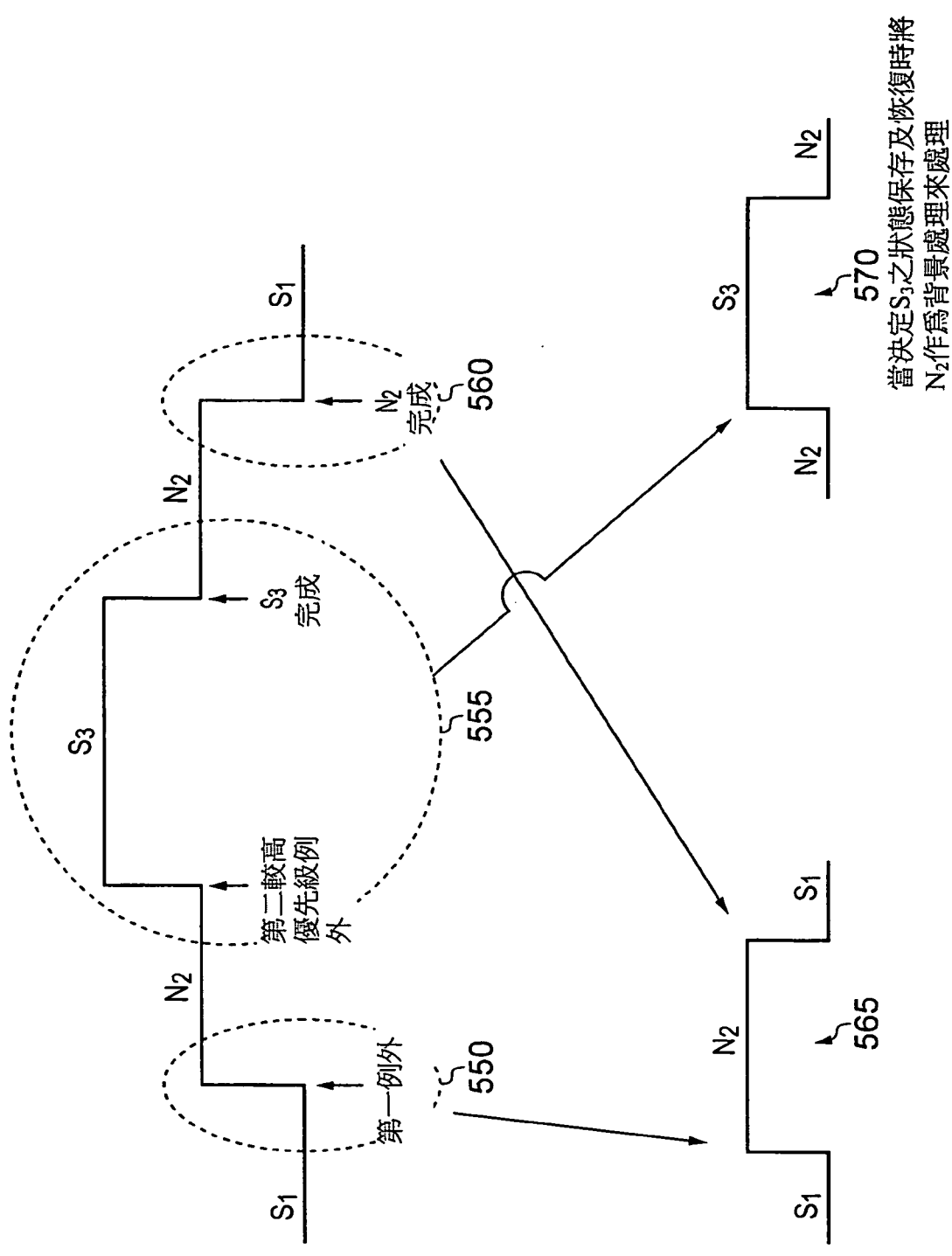
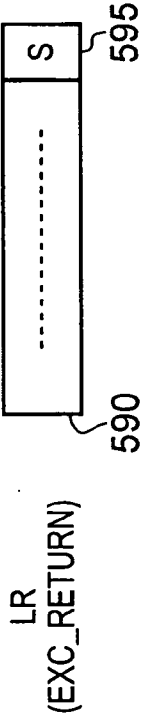


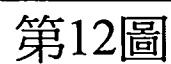
圖 9B

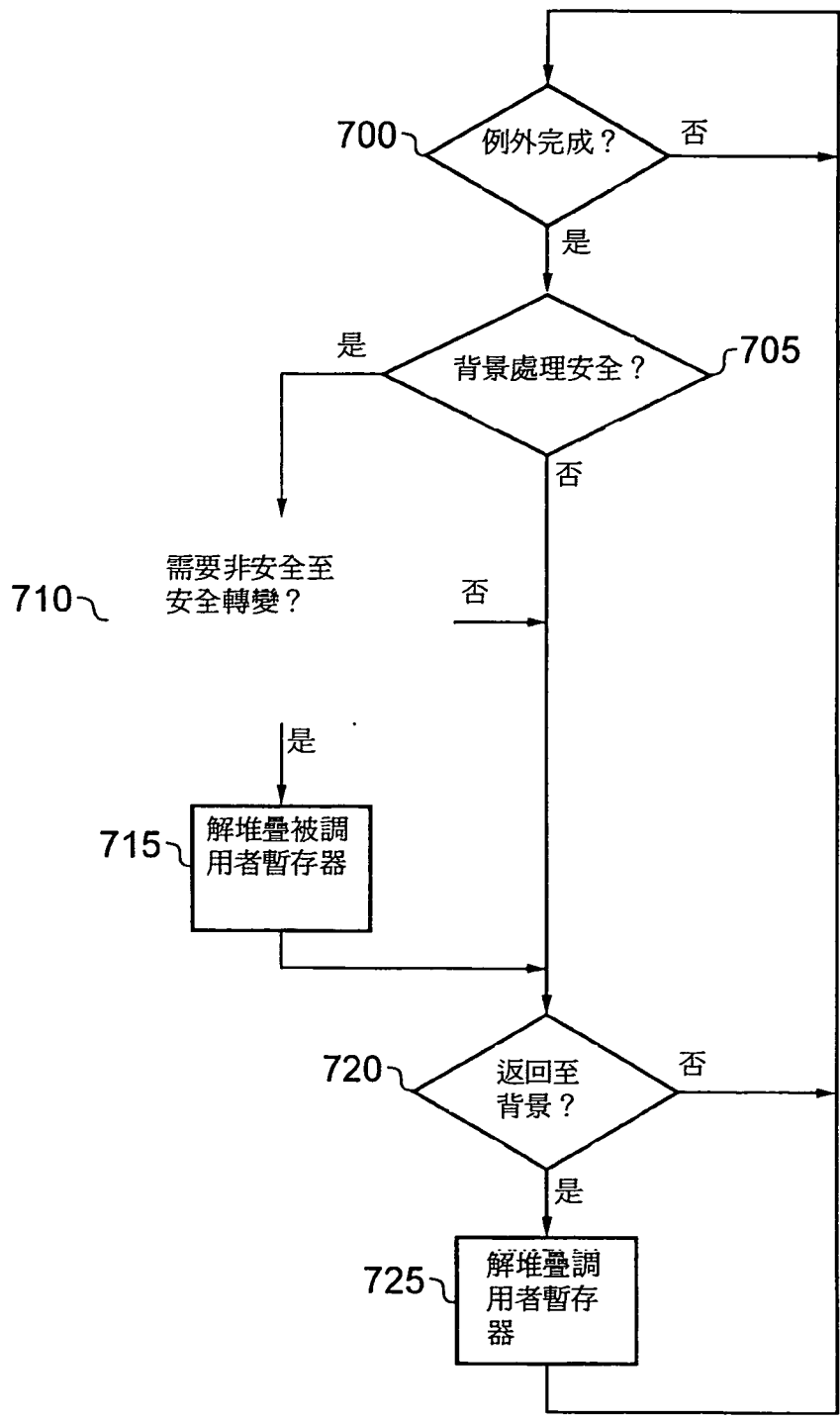


第10圖



第11圖





第13圖