



IAR Systems 安全解決方案搭配NXP MCU 實現最佳IP 保護

IAR Systems
FAE, 蔡本中 Ben Tsai
2021/8/31

Agenda

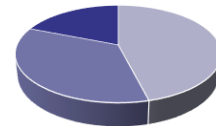
- IAR Systems 公司及產品介紹
- IAR Embedded Workbench 優異的最佳化和除錯能力
- IAR Systems 安全保護解決方案
- 應用IAR 安全解決方案於NXP LPC55S69-EVK
- Demo

IAR Systems 公司及產品介紹

IAR Systems - 嵌入式開發工具的領導者

- 總部: 瑞典 烏普薩拉
- NASDAQ 斯德哥爾摩上市
- 設立於1983年、全球14間分公司、40+國銷售
- 台灣銷售近20年、2020/4/1台灣分公司正式直接營運
- 台北辦公室位於信義區國貿大樓

Employees IAR Systems



- Product / Development
- Sales / Market / Support
- Administration

Europe

5 offices
138 employees



Asia

5 offices
26 employees



America

4 offices
38 employees



來自世界各地及跨領域的客戶群

Our products are used by many of the world's largest corporations as well as thousands of small and medium-sized companies in a range of industries, such as the automotive industry, industrial automation, medical technology, consumer electronics and the Internet of Things.

工業自動化
醫療器材
穿戴式產品
消費性電子
車用電子
IoT 產品



IAR EMBEDDED WORKBENCH IN THE CUSTOMERS' PRODUCT DEVELOPMENT

All digital products have an embedded system controlled by one or more processors.



Before a processor can be used in a product, it needs to be programmed with the correct instructions.



Product developers use IAR Embedded Workbench to program the processor and give it the correct instructions to control the finished product.



Once the processor has been programmed, it is ready for the finished product.

1 million customer products

46,000 customers

150,000 technology users

95% recurring customers

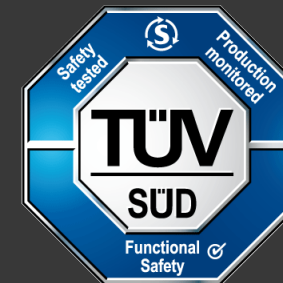


Embedded Workbench for ARM and NXP device support

- 32-bit device
 - NXP i.MX, i.MX RT CrossOver, Kinetis, LPC 系列
- 64-bit device
 - NXP i.MX 8M, i.MX 8M Mini, and i.MX 8M Nano 系列
- 功能安全版
 - NXP S32K 系列等(車用)
- **安全解決方案(Embedded Trust/C-Trust)**
 - K22/K24, KV56/KV58, K64/K65/K66, LPC55S16, LPC55S28, **LPC55S69**, i.MX RT1064
- EWARM-EXT 能編譯32/64 bit NXP MCU

The advertisement features a background of a modern office with blue and yellow lockers. Overlaid on this is a screenshot of the IAR Embedded Workbench software interface, showing various development tools like the IDE, debugger, and peripheral view. The text "Need more bits? Extend your reach!" is prominently displayed in white. A large white "64" is positioned on the right side, indicating 64-bit support. The IAR Systems logo is in the top right corner. At the bottom left of the software interface, there is a section titled "產品 A" (Product A) showing three processor models: Cortex-A (64 bit), Cortex-A (32 bit), and Cortex-M. Below this, a monitor icon displays "EW-EXT" next to a server rack icon.

通過認證的功能安全版本開發工具



- 嵌入式系統日趨複雜，功能安全認證要求與日俱增
- 系統開發工具亦列入功能安全認證的範圍內
- 開發工具本身所需的工作量非常可觀
- **IEC 61508**
Functional Safety of Electrical/Electronic/Programmable Electronic Safety
- **ISO 26262 – Automotive/Road Vehicle** 
- IEC 62304 - Medical Device Software
- EN 50128 - Railway Applications

EWARM 8.50

- IEC 60730 for Household Appliances
- ISO 13849 and IEC 62061 for Machinery Control Systems
- IEC 61511 for Process Industry
- ISO 25119 for Agriculture and Forestry

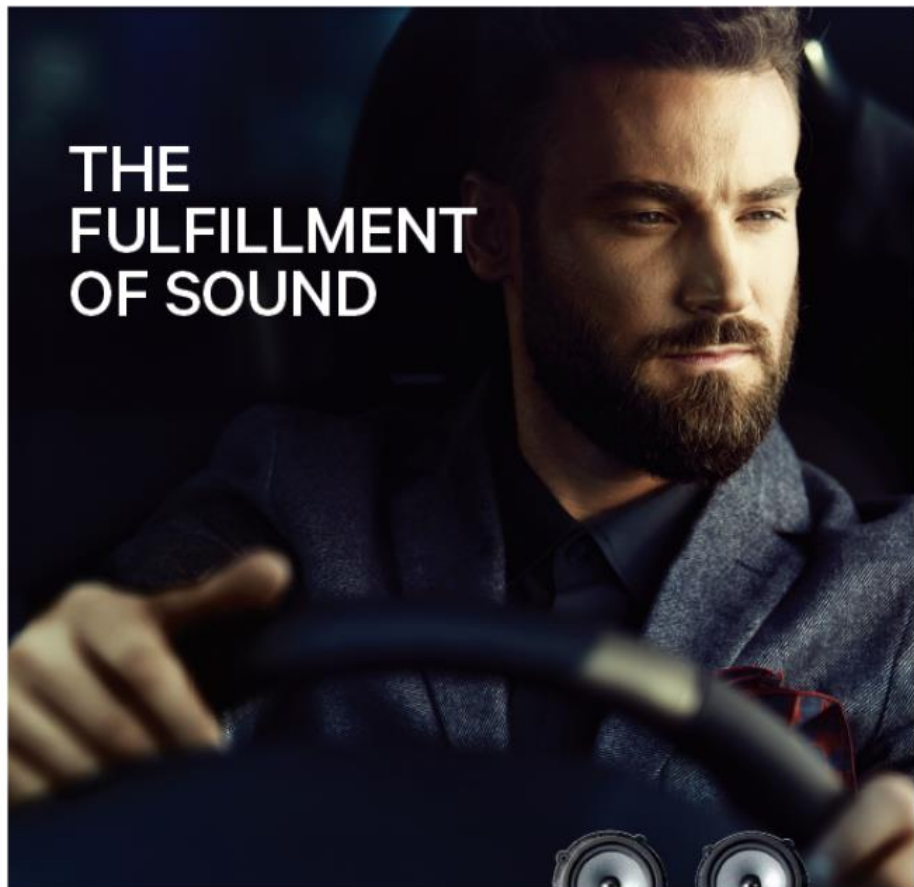
*** IAR Embedded Workbench for Arm V8.50**
IAR Embedded Workbench for RISC-V V1.40
IAR Embedded Workbench for RX V4.14
Available for : **IAR Embedded Workbench for RL78 V3.10.2**
IAR Embedded Workbench for RH850 V1.40.3
IAR Embedded Workbench for STM8 V3.11



NXP & IAR Systems – 全球白金合作夥伴

[PRODUCTS](#)[KNOWLEDGE](#)[INVESTORS](#)[ABOUT](#)

THE FULFILLMENT OF SOUND



MOBIS:
**PREMIUM IN-CAR
AUDIO SYSTEM**



Increasing work efficiency

Hyundai Mobis has introduced IAR Embedded Workbench, an integrated development environment (IDE) from IAR Systems, for high-quality sound system design in order to build an optimal infotainment system.

The Sound Engineering Team at Hyundai Mobis was able to increase the efficiency of their work by the advantage of the user-friendly and intuitive IAR Embedded Workbench.

IAR Embedded Workbench is faster than any other integrated development environment on the market today, which helps to reduce development time.

*"We selected the **NXP S32K device**, a cost-effective option, as the next generation platform and **IAR Embedded Workbench**, optimized for the Arm core, which is reliable and supports a variety of functions all bundled with fast and professional technical support to speed up development."*

- Engineer, Sound Engineering Team at Hyundai Mobis

來自客戶(Hyundai Mobis)滿意的肯定

General

I.MX Series

I.MX RT CrossOver Series

Kinetis Series

LPC Series



Automotive

S32K Series



產品開發之路: IAR始終相隨

嵌入式 開發工具

> Compiler and
debugger tools

提升程式品質

> Analysis tools

功能安全認證

> Pre-certified
build tools

持續性整合

> Linux build and
analysis tools

嵌入式安全保護

> Security from
Inception

IAR SYSTEMS VALUE OFFERING

We aim to make it possible for our customers to
create the best possible products with our tools.



SUPERIOR TECHNOLOGY

Our technology enables the best
possible product development.



A DEDICATED TEAM

We help the customer to be
an expert in their area.



FUTURE-PROOF PRODUCT DEVELOPMENT

We aim to be a supplier for
future-proof product development.

IAR Embedded Workbench

優異的最佳化和除錯能力

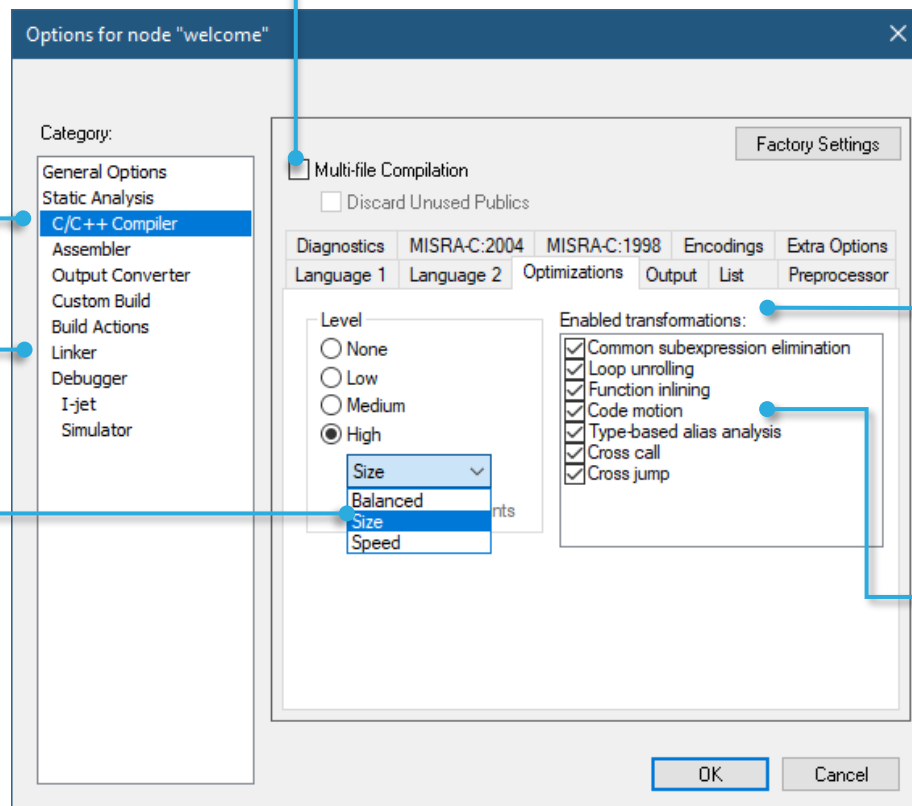
IAR C/C++ 編譯器優化

提供多組優化等級、專注於代碼大小或運行速度的解決方案

連接器可移除未使用的代碼

最佳化速度的選擇，可以不受代碼大小限制

多檔案編譯允許優化器對更大的代碼集合進行優化



優化器的主要功能可以單獨控制

通過為代碼的不同部分設置不同的優化，在大小和速度之間取得平衡

程式語言標準

- ISO/IEC 14882:2017 (C++17)
- ISO/IEC 9899:2018 (C18)
- ANSI X3.159-1989 (C89)
- IEEE 754 standard for floating-point arithmetic

廣泛地測試驗證

商業測試套件

- Plum-Hall Validation test suite
- Perennial EC++VS
- Dinkum C++ Proofer

內部開發的測試套件

- >500,000 行 C/C++ 測試代碼被反覆執行
- 處理器模式
- 記憶體模式
- 優化等級

程式碼最佳化 – 魚與熊掌兼得 (Size↓ + Speed↑)

- Option > C/C++ Optimizations > Level > High > Size
- Function Profiler > #pragma
 - #pragma optimize=no_size_constraints

IAR_DevCon_Arm - IAR Embedded Workbench IDE - Arm 8.42.2

File Edit View Project Security Debug Disassembly I-Jet Tools Window Help

Workspace Optimization - Debug

Files

- IAR_DevCon_Arm
 - Application - Debug ✓
 - Bootloader - Debug ✓
 - C-SPY Macro - Debug ✓
 - C-STAT - Debug ✓
 - Library - Debug ✓
 - Optimization - Debug ✓
 - App
 - Board
 - Startup
 - Output
 - Optimization.map
 - Optimization.out

Optimization.map core_main.c core_state.c

```
175
176     The state machine will continue scanning until either:
177     1 - an invalid input is detected.
178     2 - a valid number has been detected.
179
180     The input pointer is updated to point to the end of the token.
181 */
182 #pragma optimize=no_size_constraints
183 enum CORE_STATE core_state_transition
184 {
185     ee_u8 *str="instr;
186     ee_u8 NEXT_SYMBOL;
187     enum CORE_STATE state=
188     for( ; *str && state !=
189         NEXT_SYMBOL =
190         if (NEXT_SYMBOL ==
191             str++;
192             break;
193     )
194     switch(state)
195     {
```

Terminal I/O

Output: Log file: Off

```
2K performance run parameters for coremark.
CoreMark Size      : 666
Total ticks         : 838829470
Total time (secs)  : 13.106710
Iterations/Sec     : 152.593590
Iterations         : 2000
Compiler version   : IAR ANSI C/C++ Compiler V8.42.
Memory location    : STACK
```

Function Profiler

Function PC Samples PC Samples (%)

core_state_transition	33508	21.1
core_list_find	23200	14.5
matrix_mul_matrix_bitextract	18389	11.3
crcu8	18305	11.2
core_list_reverse	14561	9.0
matrix_mul_matrix	12850	8.0

Debug Log

CoreMark 1.0 Benchmark - ARM: ST STM32F407VG (Cortex-M4) 64 MHz, EWARM ver. 9.10.2

Level	Code (byte)	Data (byte)	Total (byte)	Size ratio	CoreMark/MHz	Speed ratio
None	18,173	1,561	19,734	1.00	1.10129	1.00
Low	17,737	1,563	19,300	0.98	1.258277	1.14
Medium	17,087	1,038	18,125	0.92	1.581696	1.44
High > Balance	16,787	1,038	17,825	0.90	2.211457	2.01
High > Speed	20,607	1,038	21,645	1.10	3.45157	3.13
High > Size	16,579	1,038	17,617	0.89	2.100296	1.91
High > Size + pragma	16,655	1,036	17,691	0.90	2.418866	2.20
High > Size + pragma + Multi-file	16,587	1,042	17,629	0.89	2.440968	2.22

全方位除錯功能

程式碼和反組譯程式碼窗口

- 類C的巨集語言
- 內置模擬器
- RTOS內核識別
- 程式碼跟踪(Trace)

The screenshot displays the IAR Embedded Workbench IDE interface for RISC-V 1.11.1. The main window shows the C source code for 'corelexip_welcome.c'. The 'Registers' window on the left lists PWM-related registers. The 'Disassembly' window on the right shows the corresponding assembly instructions. The 'Stack' window on the far right shows the current stack frame for 'main'. The 'Watch' window shows expressions like 'r', 'g', and 'b' with their current values. The 'Locals' window shows local variables like 'i', 'r', 'g', 'b', 'now', and 'then'. The 'Breakpoints' window at the bottom shows set breakpoints in the source code.

Stack 使用情況分析

表達式監控

變數監控

程式碼和數據斷點

程式碼檔/專案和工作區管理

暫存器

半主機模式 I/O視窗

靜態/動態分析工具

靜態分析工具 C-STAT - 用業界標準檢視程式碼的合規性

MISRA C:2004, MISRA C++:2008 and MISRA C:2012

Common Weakness Enumeration (CWE) and a subset of CERT C/C++

- 靈活的編碼準則選擇，直觀且易於使用
- 支持導入/導出編碼準則，維持開發團隊程式碼品質一致性
- 輕鬆產生HTML報告，檢查列表以及圖表一目了然
- 合理的價格

動態分析工具 C-RUN – 找到在寫程式時無法找出的錯誤

Bounds checking, arithmetic, heap and memory leaks checking

- 只需進行規則檢查，即可輕鬆進行初始設置
- 不用事先設置任何斷點，運行時自動檢測發現錯誤的相對應程式碼
- 合理的價格

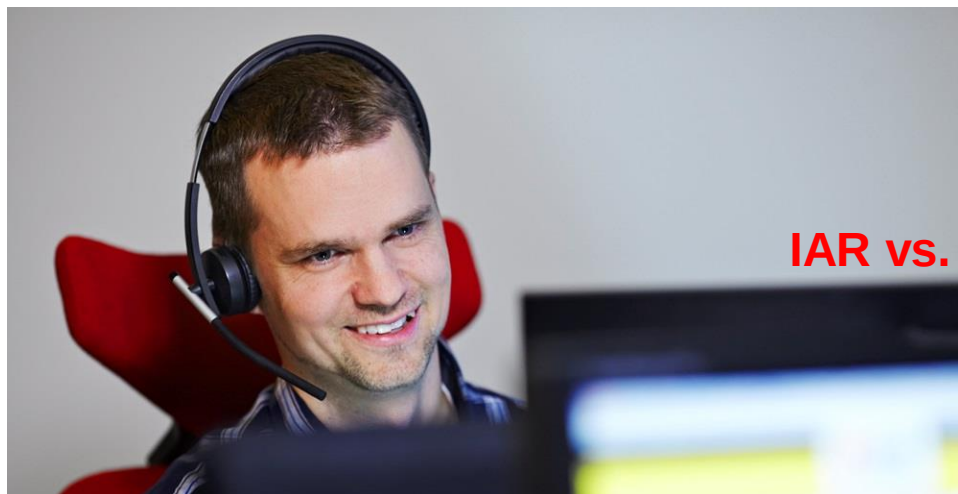
The screenshot displays the IAR Embedded Workbench IDE. The main workspace shows a project named 'GPIO_IOToggle' with source files like 'stm324xx_hal_gpio.c'. A 'C-STAT Messages' window is open, showing a list of warnings. One warning is highlighted: 'ARR-inv-index-ptr-pos' with a severity of 'Medium'. The 'C-STAT Messages' window also shows a summary report for 'ADC_DMA_Transfer' with a bar chart of messages by severity.

專門分類軟體漏洞與缺陷的「通用缺陷列表」(Common Weakness Enumeration, CWE)，在上個月列出了2019年最危險的25個軟體錯誤：2019 CWE Top 25，名列第一的是在記憶體緩衝區界限內操作的不當限制。而這也是CWE最近8年來首度更新該列表。

IAR Systems 在台原廠技術服務支援

- 軟體品質和技術支援

- IAR 珍惜使用者的開發時間，迅速提供驗證過的問題解決方法，而非自行Google 或於 Stack Overflow 等網站尋找解答
- IAR 通過Plum-Hall，Dinkumware和Perineal 等多個商業測試套件的測試
- 在13 個國家於不同時區、不同語言提供最直接的技術支援
- 定期舉辦Hands-on 訓練課程，協助用戶快速上手EWARM



IAR vs. GCC

← → ↻ Secure | <https://gcc.gnu.org/faq.html#support> ☆ 🔴 🔵

How do I get a bug fixed or a feature added?

There are lots of ways to get something fixed. The list below may be incomplete, but it covers many of the common cases. These are listed roughly in order of decreasing difficulty for the average GCC user, meaning someone who is not skilled in the internals of GCC, and where difficulty is measured in terms of the time required to fix the bug. No alternative is better than any other; each has its benefits and disadvantages.

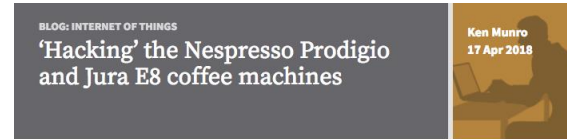
- **Fix it yourself.** This alternative will probably bring results, if you work hard enough, but will probably take a lot of time, and, depending on the quality of your work and the perceived benefits of your changes, your code may or may not ever make it into an official release of GCC.
- **Report the problem to the GCC bug tracking system** and hope that someone will be kind enough to fix it for you. While this is certainly possible, and often happens, there is no guarantee that it will. You should not expect the same response from this method that you would see from a commercial support organization since the people who read GCC bug reports, if they choose to help you, will be volunteering their time.
- Hire someone to fix it for you. There are various companies and individuals providing support for GCC. This alternative costs money, but is relatively likely to get results.

GCC: 自行修復或等待善心人士的幫忙

IAR Systems 安全保護解決方案

真實世界所發生的安全威脅

- 想喝咖啡先繳贖金，研究員綁架智慧咖啡機揭 IoT 設備資安隱憂
 - 咖啡機一啟動後就會開始連接Wi-Fi，過程中幾乎沒有任何加密、授權或驗證程序。咖啡機還缺乏任何形式的安全保護，使得所有能夠取得咖啡機IP位置的人都可以控制它
- Jeep Cherokee hacking
 - 遠程完全控制聯網車輛
(<https://youtu.be/MK0SrxBC1xs>)
- Home IoT hacking, CCTV
 - 新加坡家庭閉路電視遭到駭客入侵，損害發生在新加坡，但也發生在泰國、韓國和加拿大

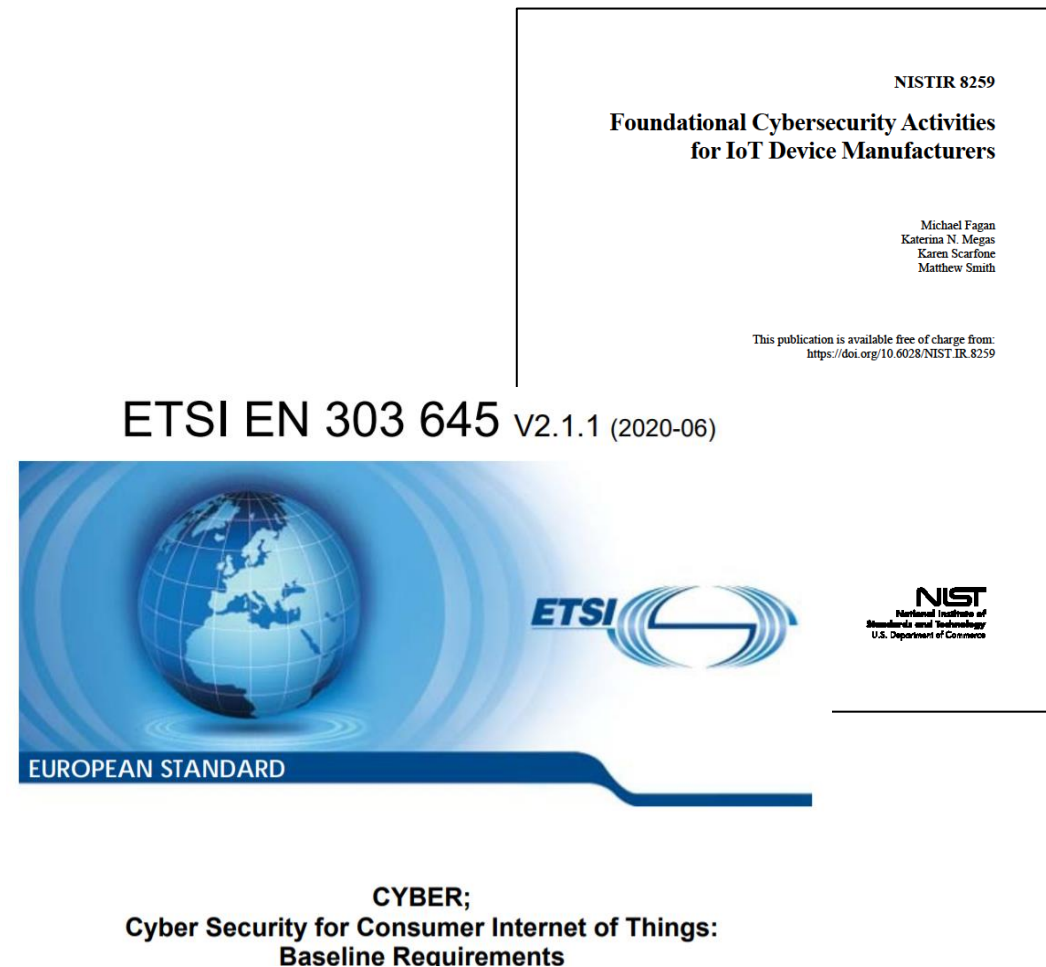


You'll probably know by now that I have a particular interest in the security of IoT coffee machines and tea kettles. Sometimes security is so poor that we have to laugh. Such simple security issues.



各國政府如何立法規範保障安全

- 歐盟領先全球於 2020 年 6 月底透過 ETSI 發佈了第一個全球適用的消費型物聯網資安標準 EN 303645 :
 - 將落實成為進入歐盟市場的物聯網設備都必須通過的標準
- 英國 UK Department of Digital (DCMS) – June 2018
 - 13 項安全設計：提高消費者互聯網的網路安全報告中，規範消費物聯網產品和相關服務安全行為準則
- 美國 US Government
 - 美國於 2020 年 12 月 4 日正式施行聯邦《物聯網網路安全法》
 - 針對美國聯邦政府未來採購物聯網設備 (IoT Devices) 制定了標準與架構



IAR 提供最完善軟體層級的安全保護

IAR 安全保護解決方案保護您的智慧財產IP 免於遭受竊取、產品仿冒、製造生產過剩等威脅

– Embedded Trust

- 使得安全開發人員建立SBM、密鑰和憑證的信任鏈



– C-Trust

- 使得程式開發人員都能交付安全、加密的應用程式



– Secure Desktop Provisioner

- 安全指配器簡化原型/批量安全生產



– IAR Embedded Workbench

- 完整的C/C++ 編譯和除錯工具鏈之集成開發環境



– C-STAT

- 集成在開發工作流程中的靜態程式碼分析工具



– I-jet

- 業界領先的高速除錯器



IAR INCEPTION SUITE
安全解決方案

NXP 提供最佳硬體層級的安全保護

- NXP 提供安全保護最重要的信任根(Root of Trust)
 - 無需自行產生隨機的ID 或是使用Device ID，使用最新無法複製的物理特性功能(PUF)



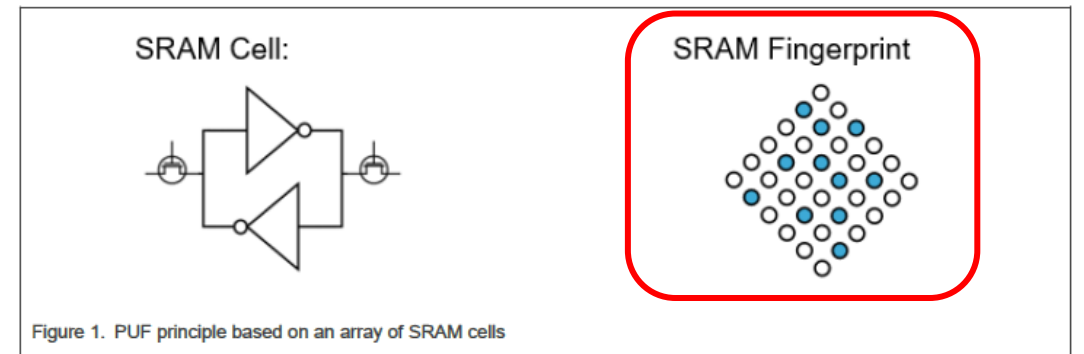
↓ 馬 → 花紋



↓ 人 → 指紋



↓ MCU → PUF
(SRAM “指紋”)

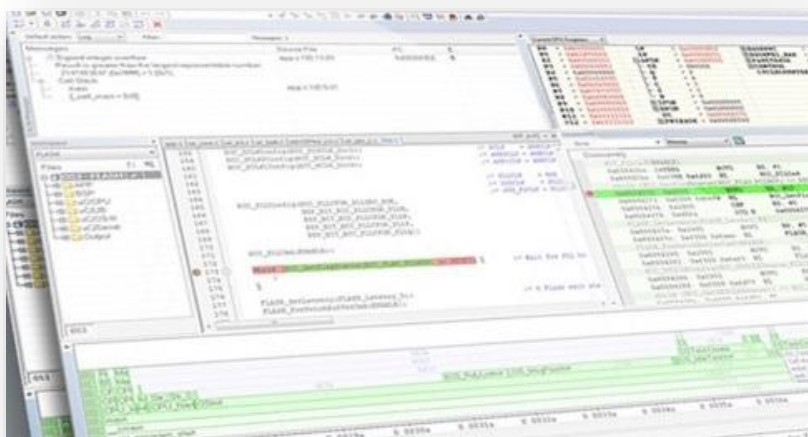


安全開發工作流程簡介

傳統軟體開發流程



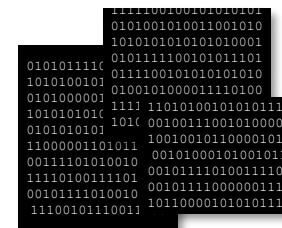
設計應用程式和編碼開發



建置和除錯應用程式



發行映像檔(image)
進行量產



安全開發工作流程

開發安全內文
(Secure Context)

建置安全啟動
管理器 SBM,
指配設備

開發應用
程式

測試

部署

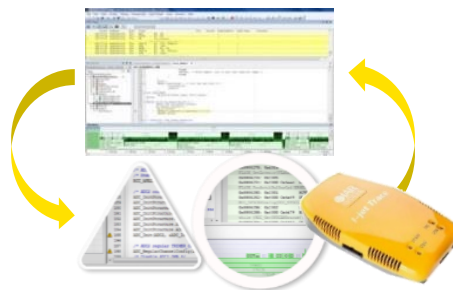
生產
製造

管理
維護

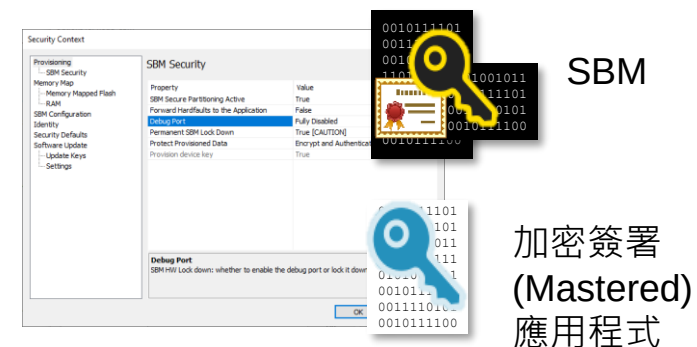
創建安全內文，構建安全啟動管理器(Secure Boot Manager, SBM)並指配(Provision)設備



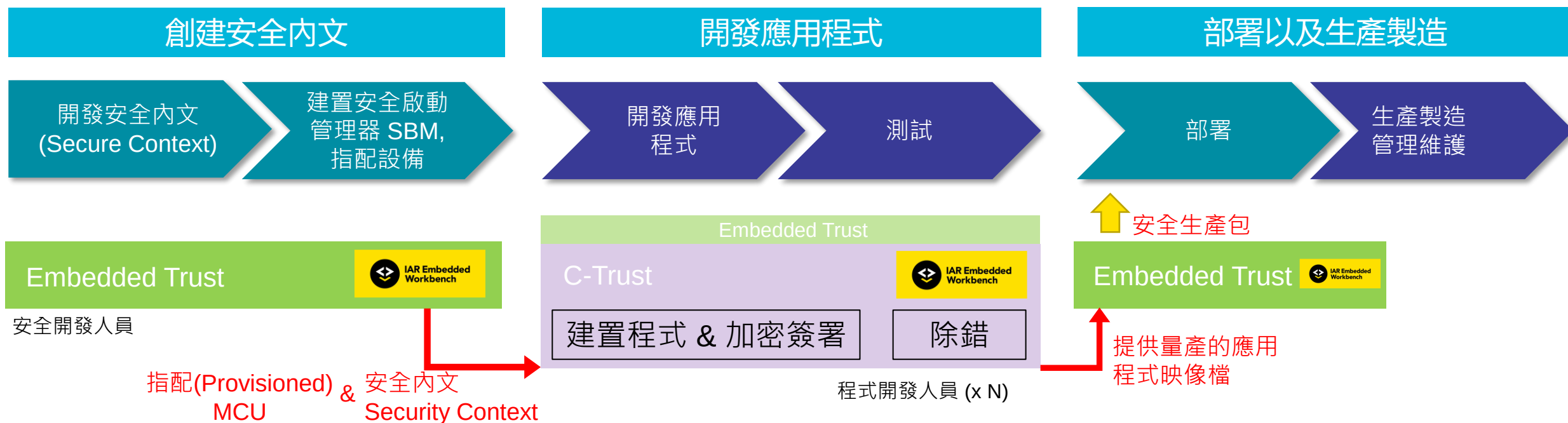
使用開發密鑰開發和測試應用程式



由部署到製造使用生產密鑰構建流程



使用Embedded Trust 和 C-Trust

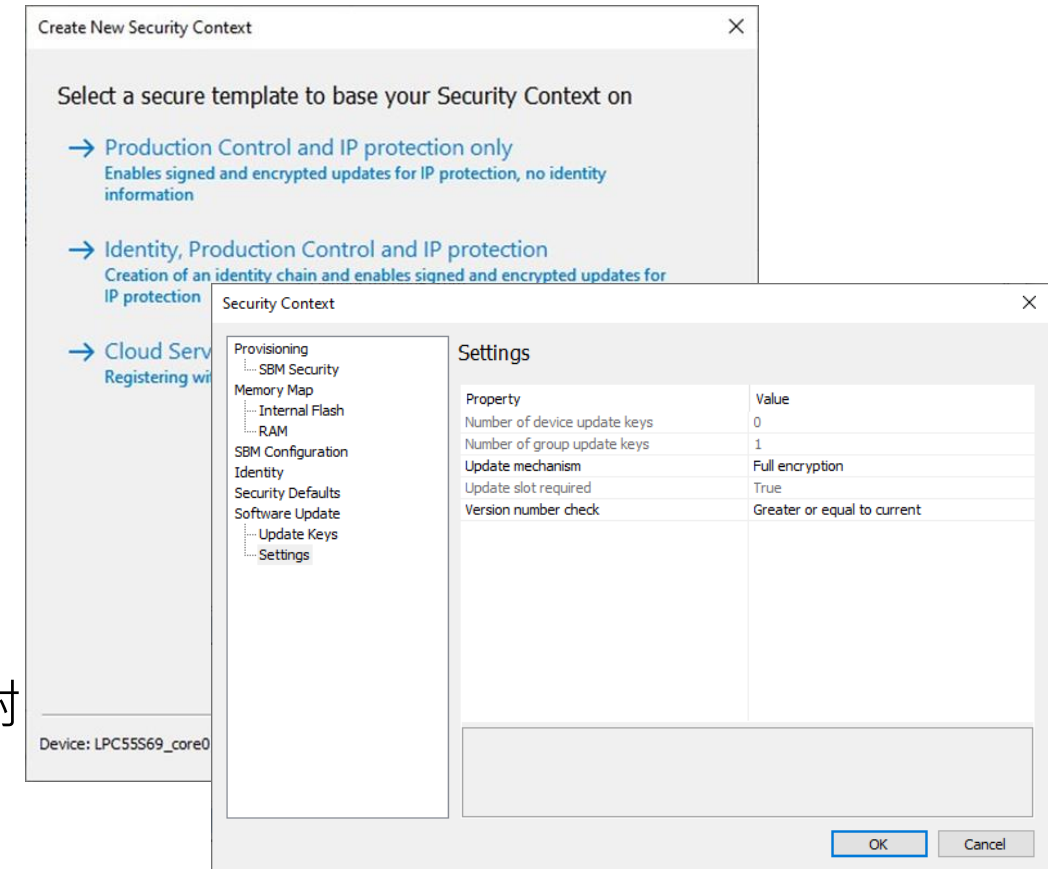


- **Embedded Trust** 提供由安全內文到安全生產包生成的完整流程，包括安全啟動管理器的創建以及應用程式的開發
- **C-Trust** 提供Embedded Trust 功能的子集合, 專注於應用程式開發階段和整個產品開發週期的評估

使用Embedded Trust 創建安全內文以及安全啟動管理器

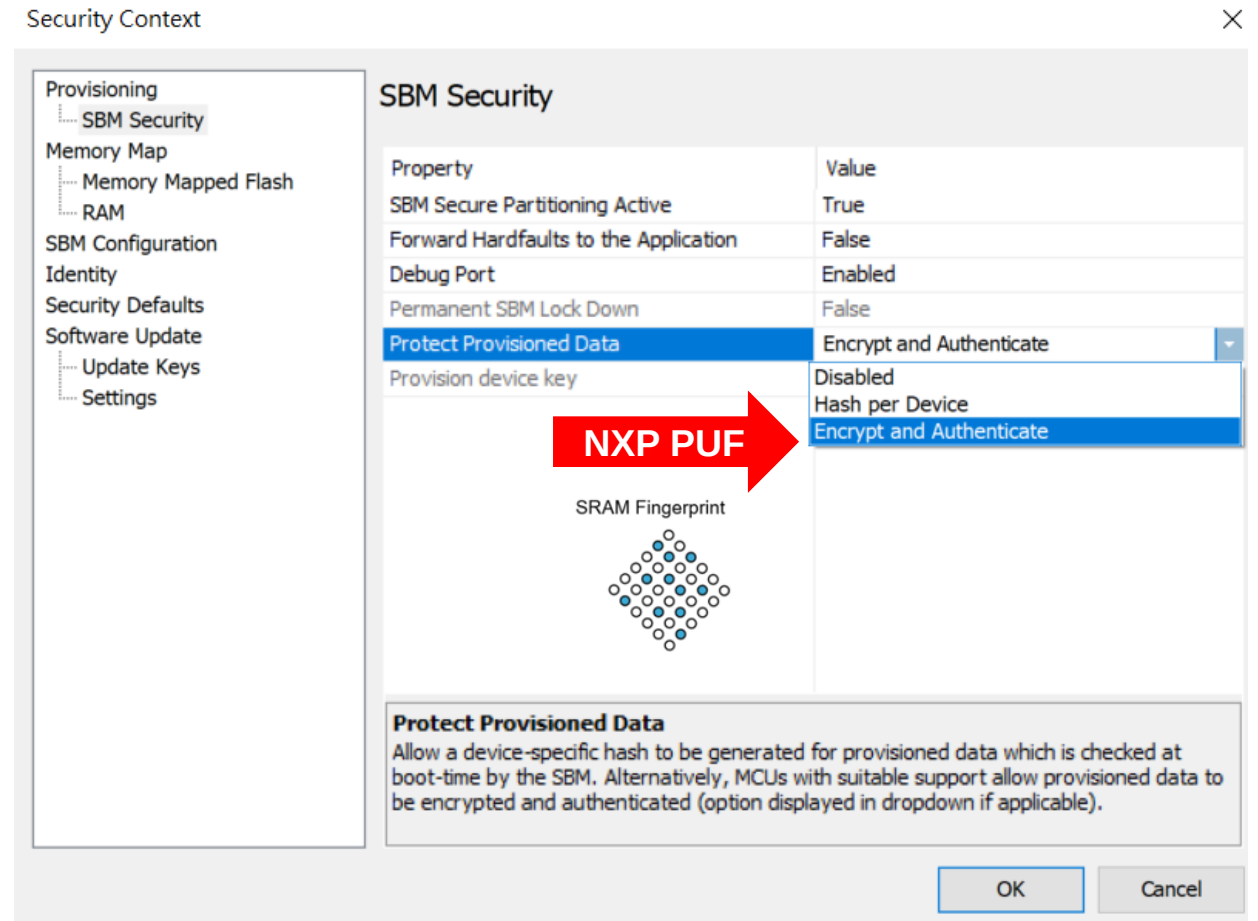
安全內文(Security Contexts)

- 保護應用程式所需安全環境的描述內容
- 屬性包括：
 - 加密密鑰和憑證
 - 安全啟動配置
 - 設備安全
 - 應用程式更新流程和機制
 - 設備內存分配
- **Embedded Trust** 提供精靈來協助您手把手地創建和配置安全內文
 - 包括生成適當的安全啟動管理器專案
 - 注意：**C-Trust** 無法創建新的安全內文（因為它是針對應用程式開發的）



NXP PUF 的支援為各種應用程式提供增強防護

- Embedded Trust 最新版本1.53 已支援NXP PUF
- 配置安全內文啟用NXP PUF
 - 於Protect Provisioned Data (保護指配資料)的選單中，選取Encrypt and Authenticate (加密和身份驗證)
 - 使用 MCU 特定的安全技術(例如NXP PUF) 在指配(provisioning) 時保護數據
 - 安全啟動管理器(SBM) 可以在運行時從安全存儲中恢復受保護的指配數據



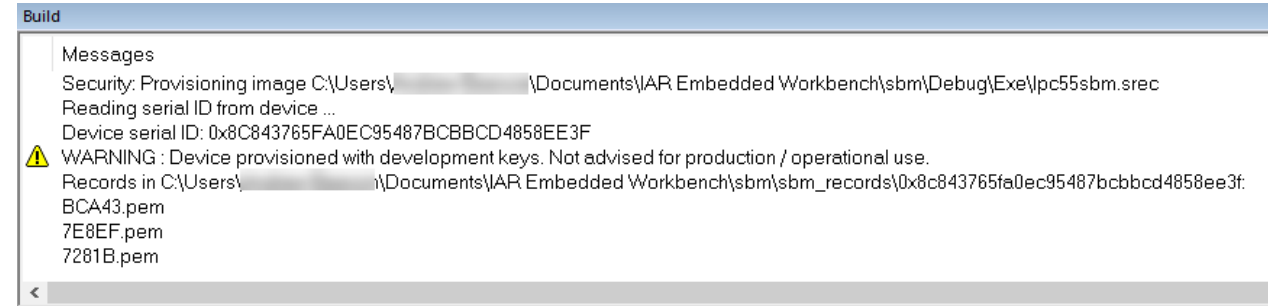
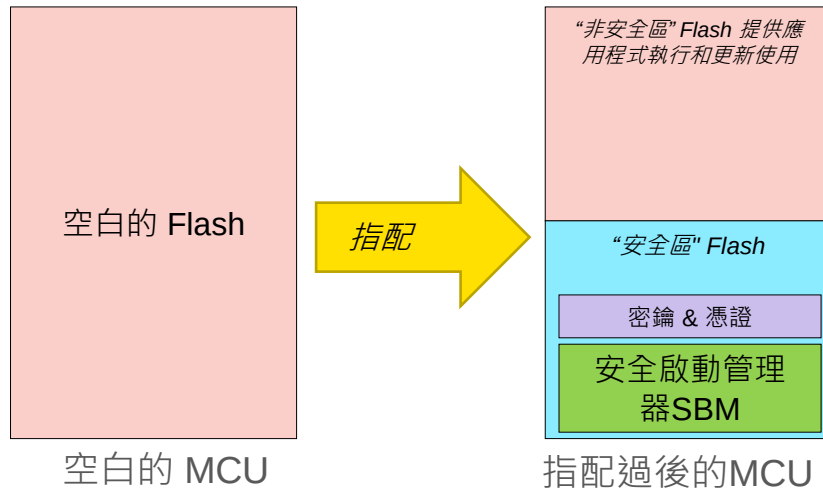
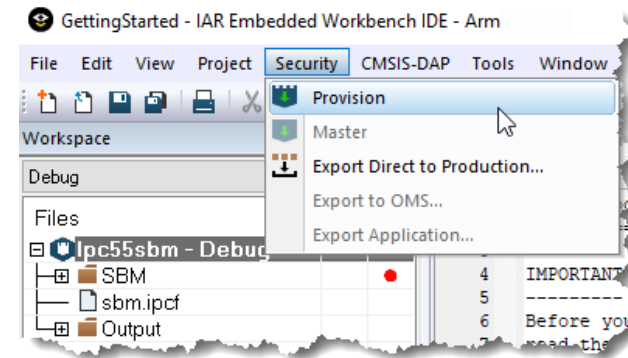
安全啟動管理器Secure Boot Manager (SBM)

- 為 MCU 提供強大的信任根(Root of Trust)
 - 保護整個啟動過程
 - 保護 MCU 免受惡意軟體侵入
 - 啟用安全更新機制
- 經由Embedded Workbench 的新專案產生精靈所建立，然後配置為安全內文的一部分
 - 提供程式碼，因此可以針對最終產品進行修改或優化
- 建置後指配至 MCU 的同時，提供安全密鑰和憑證以及配置 MCU 安全設定
 - 啟動程序是不可變的
- SBM 亦為應用程式提供完整的 ABI 介面，可由此請求安全服務



指配(Provision) MCU

- 指配(Provision)不僅僅是將 SBM 映像燒錄到Flash
 - 設備序列號將從目標中讀取並合併到設備憑證中以形成信任根的基礎
 - “指配的數據” 包括密鑰和憑證，然後與 SBM 一起被燒錄至MCU 的Flash
 - 在最終量產期間，MCU 也將受到保護 - 之後的除錯訪問將被禁止，包含 SBM 和指配數據的Flash 區域將被鎖定



安全啟動管理器SBM 以及應用程式安裝

- 任何MCU 後續的“應用程式燒錄”都必須經由使用 SBM 的安全流程進行交付，以確保主應用程式有被正確地簽署和加密
- 重置時，在運行已安裝的應用程式前，SBM 會先計算雜湊 (Hash) 並將其與存儲在簽名列表（受保護內存中）中的值進行比對，以確保應用程式在內存中的任何內容都沒有被篡改
- 亦可執行完全經過身份驗證的軟體安全更新流程
 - 應用程式的軟件更新放置在單獨的內存位置，並調用 SBM ABI 進行安裝
 - 更新完成後，進行身份驗證的啟動流程並安裝程式再加以執行
 - 可以在需要時強制執行反回滾(防止設備降級到舊版本)

```
Untitled_0*
File Edit Connection View Remote Window Help
New Open Save Connect Disconnect Clear Data Options View Hex Help

$[OEM] =====
$[OEM] SBM v0.1: Jan 26 2021 16:37:11
$[OEM] Configuration parameters:
$[OEM]   SBM_BOOT_STATUS_TRACKING: 1
$[OEM]   SBM_UPDATE_LOGGING: 0
$[OEM]   SBM_FAIL_LAUNCH_API: 0
$[OEM]   SBM_VERSION_CHECKING: 2
$[OEM]   SBM_RECORD_BOOT_TIME: 0
$[OEM]   SBM_REPORT_SBM_SIZES: 0
$[OEM]   Update: 0x58000 - 0x8ffff
$[OEM]   Executable: 0x10000 - 0x47fff
$[OEM] oem_boot_status(11) called: implementation to be supplied
$[OEM] Checking version
$[OEM] oem_boot_status(6) called: implementation to be supplied
$[OEM] Update from version 0x3010000 to 0x3010203
$[OEM] oem_boot_status(7) called: implementation to be supplied
$[OEM] Installing version 0x3010203
$[OEM] oem_boot_status(8) called: implementation to be supplied
$[OEM] Update installed
$[OEM] oem_boot_status(2) called: implementation to be supplied
$[OEM] =====
$[OEM] Checking executable signature
$[OEM] oem_boot_status(9) called: implementation to be supplied
$[OEM] Running executable image version 0x3010203

COM4 / 115200 8-N-1
Connected 00:10:51, 4433 / 0 bytes
TX RX RTS CTS DTR DSR DCD RI
```

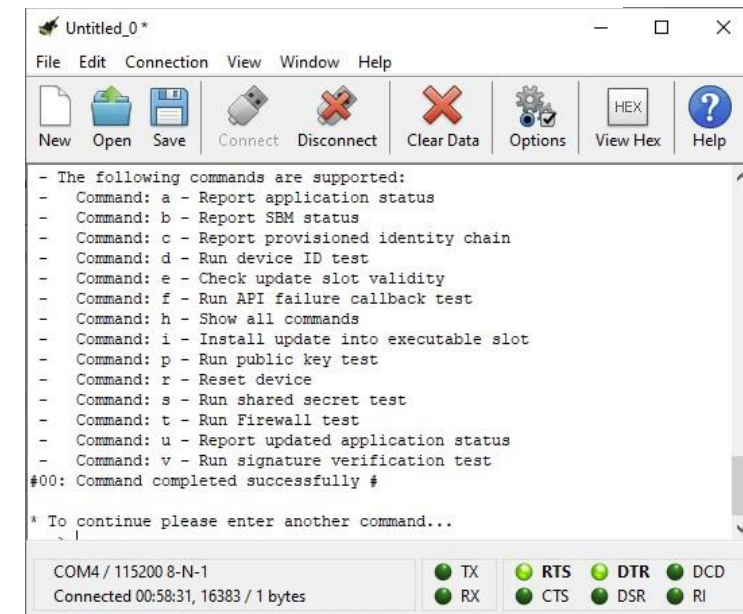
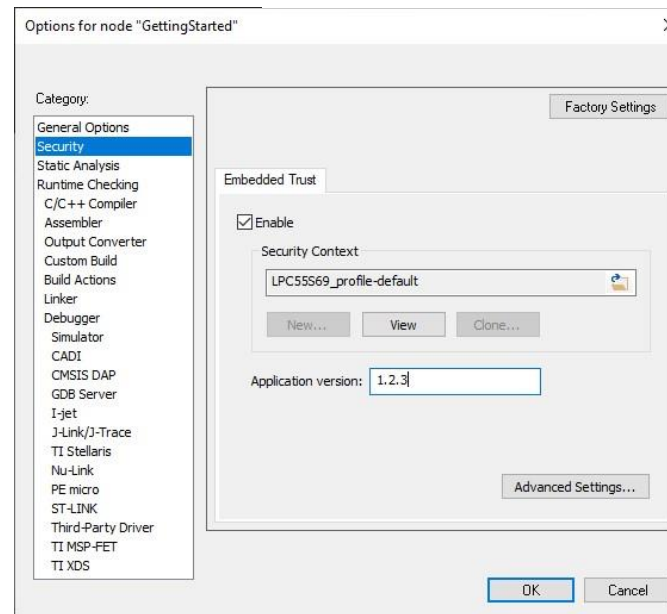
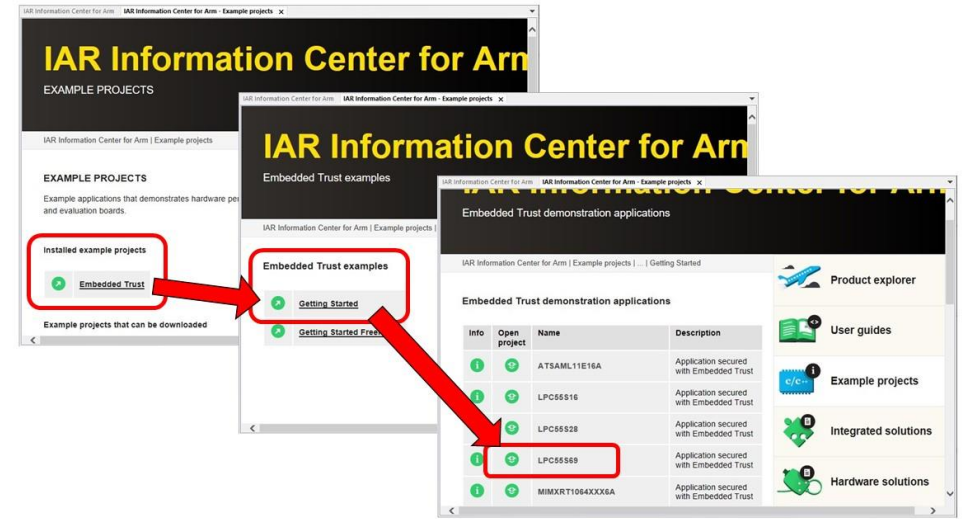
更新已安裝版本
1.2.3 > 1.0.0

在執行應用程式
前先進行驗證

使用C-Trust 開發應用程式安全保護

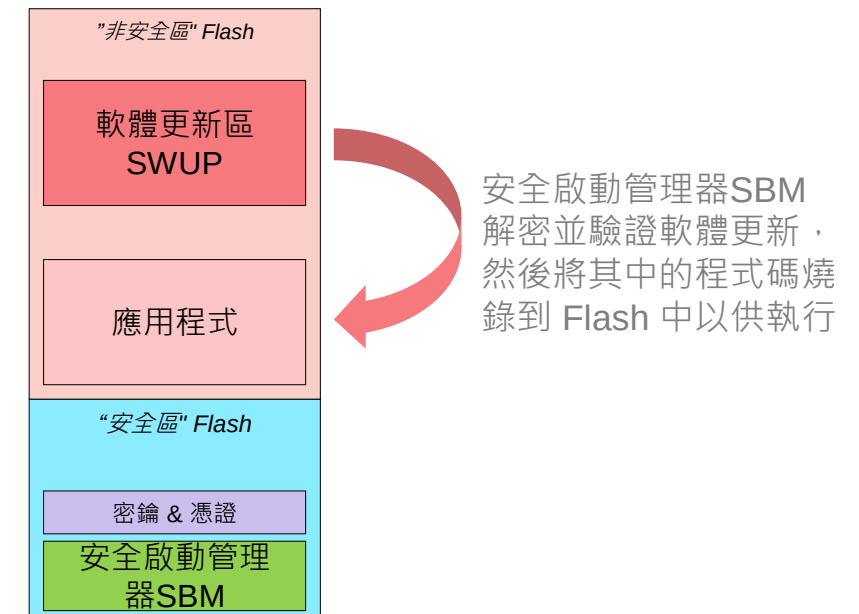
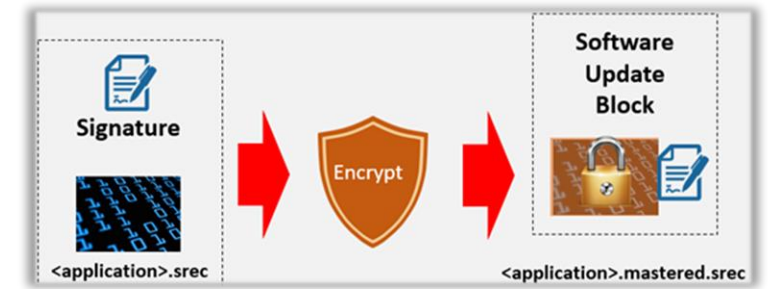
Getting Started 應用程式範例

- 為每個支持的設備提供了簡單的範例專案
 - 由Information Center 輸入專案
 - 選取安全啟動管理器所使用的安全內文
 - 給定版本
 - 建置並“加密簽署 (Master)”再燒錄至設備
- 提供一個簡單的使用者介面來使用安全啟動管理器所提供的各項安全功能
- 完全整合Embedded Workbench 的標準建置/除錯功能，可進行已加密簽署 (Master) 應用程式的除錯



加密簽署(Mastering) 應用程式

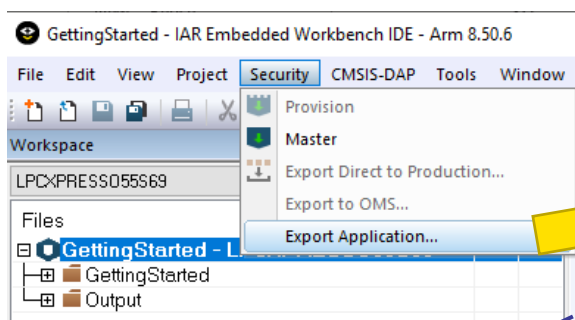
- 加密簽署(Mastering) 應用程式映像檔，使用相關安全內文中的設置，對其進行簽署和加密
 - 安全內文必須與指配給目標 MCU SBM 所使用的內文相匹配，應用程式才能被執行
- 當啟用了安全保護功能，在建置應用程式時會自動執行加密簽署(Mastering)，亦可手動執行
- 可以將加密簽署(Mastering) 的應用程式作為軟體更新 (SWUP) 燒錄到目標 MCU 上的非安全區的 Flash 中
 - 安全啟動管理器SBM 將會進行檢查、安裝並最終執行該應用程式



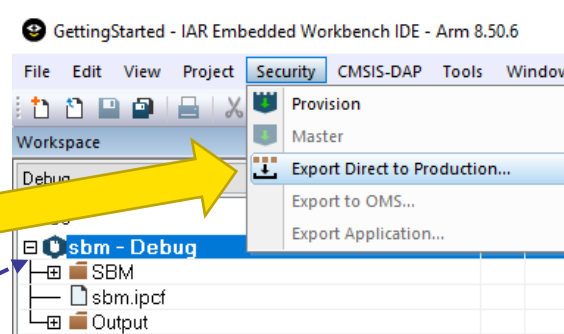
使用Secure Desktop Provisioner 導出至生產流程

導出至原型開發或最終量產流程

應用程式專案



安全啟動管理器SBM 專案



切換至生產用途的
安全內文

例如

- 禁用 SBM 紀錄輸出
- 禁用除錯訪問
- 鎖定 SBM 內存
- 切換到生產密鑰和憑證
- 應用程式版本檢查機制
- 啟用對指配數據的保護

安全設備憑證

安全設備憑證

安全生產包

安全生產包

帶有 Secure Thingz 安全設備 (HSM) 的安全指配器 (Secure Desktop Provisioner)



Secure Desktop Provisioner
安全指配器



帶有集成 Secure Thingz 安全設備 (HSM) 的批量生產系統

應用IAR 安全解決方案於 NXP LPC55S69-EVK

開發環境 - IAR Systems

- IAR Embedded Workbench for Arm (EWARM) 版本 8.50.9
- Embedded Trust & C-Trust 版本1.53
- 開發板：NXP LPC55S69-EVK
- Debugger：內建CMSIS DAP

Technical and Functional Specifications

Microcontroller	• LPC55S69 dual core Arm Cortex-M33 microcontroller running at up to 150 MHz.
Memory Expansion	• Micro SD card slot (4-bit SDIO).
Connectivity	• UART and SPI port bridging from LPC55S69 target to USB via the onboard debug probe. • High and full speed USB ports with micro A/B connector for host or device functionality.
Debug	• Onboard, high-speed USB, Link2 debug probe with CMSIS-DAP and SEGGER J-Link protocol options. • Hardware support for external debug probe.
Sensors	• NXP MMA8652FCR1 accelerometer
Audio	• Stereo audio codec with a line in/out
Expansion Options	• MikroElektronika Click expansion option • LPCXpresso-V3 expansion connectors compatible with Arduino® UNO Rev3 • PMod compatible expansion / host connector
User Interface	• RGB user LED, plus Reset, ISP, Wake, and user buttons



展演內容說明

- 使用**Embedded Trust** 創建 SBM 並指配到 NXP LPC55S69
 1. 生成安全內文和 SBM 專案
 - 成為系統不可改變的信任根
 2. 為 LPC55S69 建立和配置 SBM 和密鑰/憑證
- 使用**C-Trust** 加密簽署 (Master) 應用程式
 1. 於應用程式專案選取安全內文
 2. 加密簽署(Master) 應用程式
 3. 通過 VCOM/UART 終端機並重置目標，檢查安全啟動管理器SBM 所提供的各項安全功能



內建 CMSIS-DAP 除錯功能的
LPCXpresso55S69-EVK 板

使用Embedded Trust 創建 SBM 並指配到 NXP LPC55S69

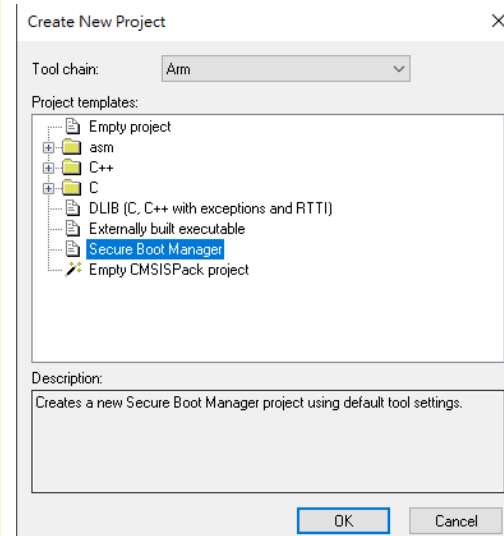
建立SBM

設定SBM

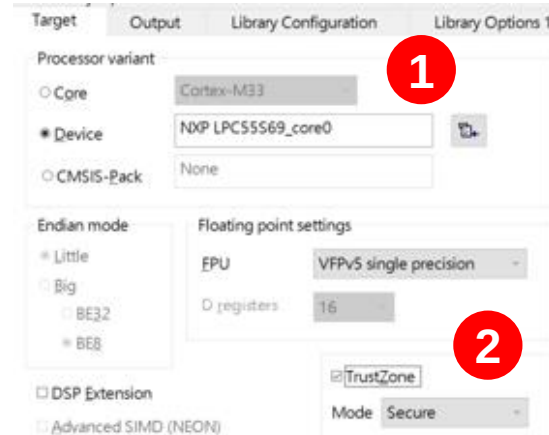
安全內文

指配

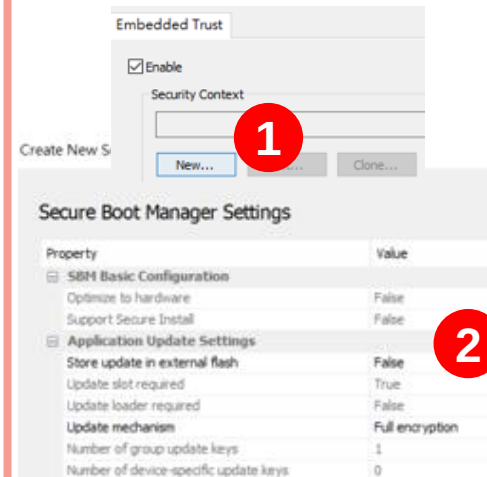
- 建立SBM專案
 - Project > Create New Project



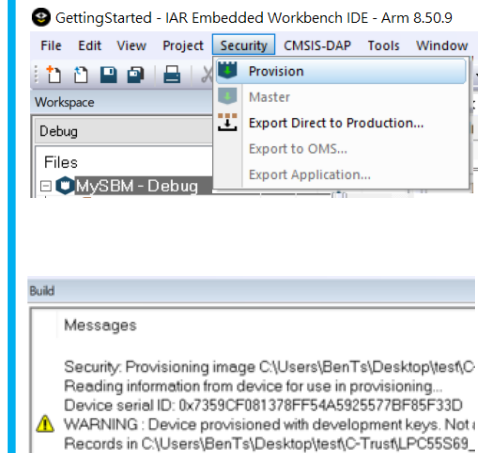
- Options > General Options > Target 頁面
 1. 選取NXP 設備
 2. 啟用TrustZone



- 啟用Security
 1. 新增安全內文
 2. 設定安全內文



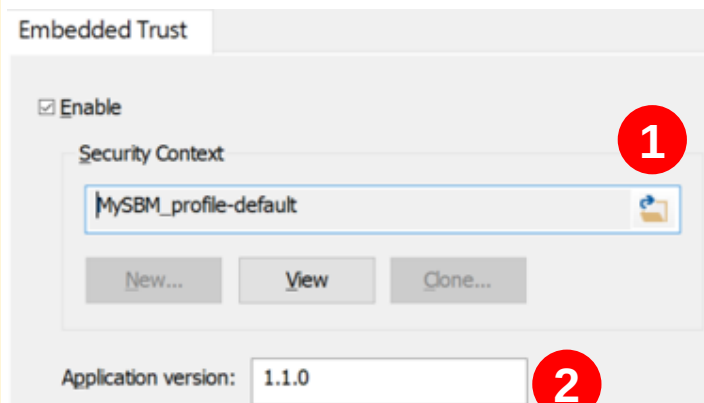
- 執行Security > Provision



- 使用C-Trust 加密簽署 (Master) 應用程式

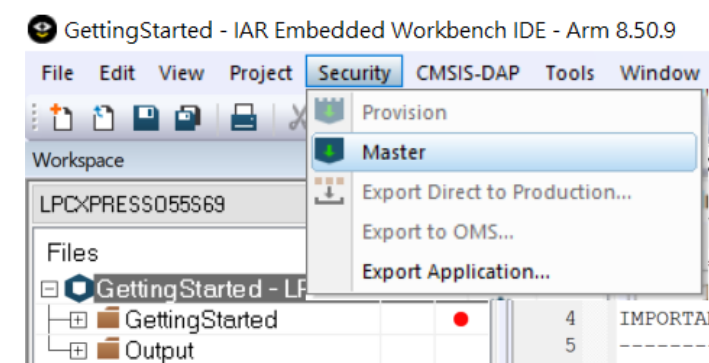
選取安全內文

- Options > Security 頁面
 1. 選取安全內文
 2. 給定應用程式版本



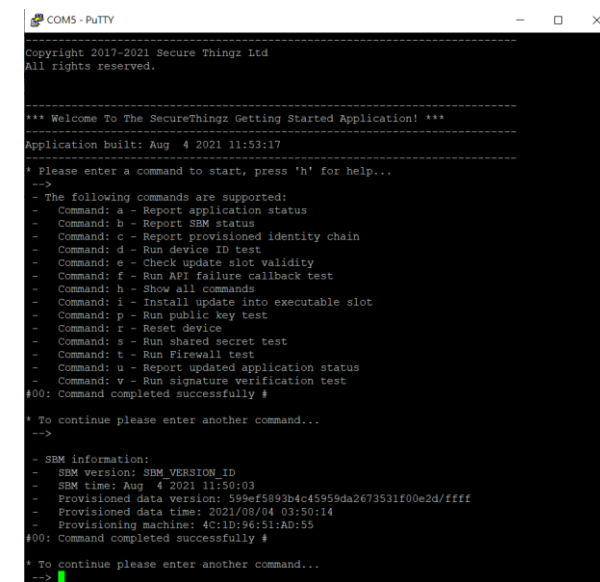
加密簽署

- 執行Security > Master



執行應用程式

- 執行Download and Debug



總結

- 由於物聯網資安問題層出不窮，各國已加緊腳步立法規範，IAR 為此提供完善的安全解決方案
- IAR 安全解決方案涵蓋初期的原型設計到最後的量產，完美整合於EWARM 開發環境
- 使用IAR 的安全解決方案搭配NXP 硬體保護功能，實現最佳的IP 安全保護

相關資料

- EWARM
 - <https://www.iar.com/iar-embedded-workbench/#!?architecture=Arm>
- Embedded Trust
 - <https://www.iar.com/products/requirements/security/embedded-trust/>
- C-Trust
 - <https://www.iar.com/products/requirements/security/c-trust/>
- Security from Inception Suite
 - <https://www.iar.com/products/requirements/security/security-from-inception-suite/>
- 視頻
 - [Getting started with C-Trust](#)
 - [Secure Desktop Provisioner with the NXP LPC55S69-EVK board](#)
- IP 保護技術文章
 - <https://www.iar.com/knowledge/learn/security/ip-protection--essential-to-protect-your-business-and-your-customers/>



Thank you for your attention!



IAR Systems 台灣分公司

臺北市信義區基隆路1段333號24樓2406室

市話：(02) 2757-6800

Email：sales.tw@iar.com

繁中入口網站：<https://go.iar.com/l/223402/2020-05-12/l9tln>

試用版安裝網站：(30天無容量限制/32 KB容量限制)

<https://www.iar.com/products/architectures/arm/iar-embedded-workbench-for-arm/iar-embedded-workbench-for-arm--free-trial-version/>

