

ISA/ IEC 62443-4-1 與 4-2 實戰應用

工控產品安全開發與實作中 常見誤解與最佳實踐


SZ Lin (林上智)

Date: 2024/05/16

2024 | IACS/ OT 資安攻擊

1.260	05/03/2024	2024	The city of Oakley, in the US state of California, declared a state of emergency after e...	United St...	Governemnt
1.259	06/03/2024	2024	Threat actors are targeting misconfigured and vulnerable servers running Apache Ha...	Global	Tecnology services
1.258	06/03/2024	2024	The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) has ann...	Canada	Financial Services
1.257	06/03/2024	2024	Apple is advising immediate patching against two critical zero-day vulnerabilities tha...	Global	Tecnology services
1.256	06/03/2024	2024	Cybercrime group GhostSec is associated with a Golang variant of ransomware calle...	Global	Public Services
1.255	07/03/2024	2024	Threat actors have been leveraging fake websites advertising popular video conferen...	Global	Information Technology s...
1.254	07/03/2024	2024	Sensitive Swiss federal government data, including classified documents and log in c...	Switzerla...	Governemnt
1.253	26/02/2024	2024	Travelers are being targeted with malware disguised as refunds from Booking.com. A...	Global	Commercial and public se...
1.252	25/02/2024	2024	Russian hackers hacked the editorial system of the Ukrainian TV channel "Priyamy," ...	Ukraine	Communication and telec...
1.251	26/02/2024	2024	The Netskope Threat Labs report highlights that the financial sector remains one of t...	Global	Banking and finance sector
1.250	26/02/2024	2024	The group behind the LockBit ransomware has reemerged on the dark web, moving ...	Global	Information Technology s...
1.249	26/02/2024	2024	Hackers are exploiting a vulnerability in a CMS editor discontinued 14 years ago to c...	Global	Education and Research s...
1.248	27/02/2024	2024	Cybersecurity researchers have discovered a vulnerability in the Hugging Face platfo...	Global	Information Technology
1.247	27/02/2024	2024	Hackers are manipulating SEO results to direct users to malicious sites, aiming to de...	Global	Information Technology s...
1.246	23/02/2024	2024	Truck and trailer rental company U-Haul stated that around 67,000 customers in the ...	United St...	Transport sector and syste...
1.245	24/02/2024	2024	Canada's national police force was hit with a cyberattack Friday that was of an "alar...	Canada	Public Services
1.244	22/02/2024	2024	Hackers managed to download 185 gigabytes of data from the central drive of the U...	Iceland	Education and Research s...
1.243	20/02/2024	2024	Russian cyber spies behind the SolarWinds breach are adapting their techniques to h...	Global	Transport sector and syste...
1.242	20/02/2024	2024	A group of hackers claimed responsibility for a cyberattack that disrupted internet c...	United Ki...	Education and Research s...
1.241	21/02/2024	2024	Foundation Health Partners, which manages three healthcare facilities in Fairbanks, w...	United St...	Chemical and Farmaceutic...
1.240	22/02/2024	2024	Pharmacies across the country are suffering from the impacts of a cyberattack on Ch...	United St...	Chemical and Farmaceutic...
1.239	14/02/2024	2024	Southern Water has warned that data belonging to 5-10% of its customers has been ...	United Ki...	Water and wastewater sec...
1.238	14/02/2024	2024	manufacturer Varta was targeted in a cyberattack that paralyzed parts of its syste...	Germany	Manufacturing and autom...

EU | on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020

EUROPEAN COMMISSION

Brussels, 15.9.2022
COM(2022) 454 final
2022/0272(COD)

Proposal for a
REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020
(Text with EEA relevance)
{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

- Reasons for and objectives of the proposal**

Hardware and software products are increasingly subject to successful cyberattacks, leading to an estimated global annual cost of cybercrime of EUR 5.5 trillion by 2021. Such products suffer from two major problems adding costs for users and the society: (1) a low level of cybersecurity, reflected by widespread vulnerabilities and the insufficient and inconsistent provision of security updates to address them, and (2) an insufficient understanding and access to information by users, preventing them from choosing products with adequate cybersecurity properties or using them in a secure manner. In a connected environment, a cybersecurity incident in one product can affect an entire organisation or a whole supply chain, often propagating across the borders of the internal market within a matter of minutes. This can lead to severe disruption of economic and social activities or even become life threatening.

The cybersecurity of products with digital elements has a strong cross-border dimension, as products manufactured in one country are often used across the internal market. In addition, incidents initially affecting a single entity or a single Member State often spread within minutes across the entire internal market.

While existing internal market legislation applies to certain products with digital elements, most of the hardware and software products are currently not covered by any EU legislation tackling their cybersecurity. In particular, the current EU legal framework does not address the cybersecurity of non-embedded software, even if cybersecurity attacks increasingly target vulnerabilities in these products, causing significant societal and economic costs. There are numerous examples of noteworthy cyberattacks resulting from suboptimal product security, such as the WannaCry ransomware worm, which exploited a Windows vulnerability that affected 200 000 computers across 150 countries in 2017 and caused a damage amounting to billions of USD; the Kaseya VSA supply chain attack, which used Kaseya's network administration software to attack over 1 000 companies and forcing a supermarket chain to close all its 500 shops across Sweden; or the many incidents in which banking applications are hacked to steal money from unsuspecting consumers.

Companies affected by this Act have 36 months to comply, facing penalties of up to **€15 million or 2.5% of global turnover for non-compliance**

CNS | 國家標準網路服務系統

CNS 62443-1-1 X6143-1-1

工業通訊網路 - 網路及系統安全 - 第1-1部：術語、概念及模型

Industrial communication networks – Network and system security – Part 1-1:
Terminology, concepts and models

狀態：現行標準 最新日期：109/12/24

版本：中文版 價格(新台幣)：390

[預覽](#) [加入購物車](#)

CNS 62443-2-4 X6143-2-4(彩色版)

工業自動化及控制系統之安全性 - 第2-4部：IACS服務提供者之安全計畫要求事項
Security for industrial automation and control systems – Part 2-4: Security program
requirements for IACS service providers

狀態：現行標準 最新日期：111/12/15

版本：中文版 價格(新台幣)：375

[預覽](#) [加入購物車](#)

CNS 62443-3-1 X6143-3-1(彩色版)

工業通訊網路 - 網路與系統安全 - 第3-1部：工業自動化及控制系統之安全技術
Industrial communication networks – Network and system security – Part 3-1:
Security technologies for industrial automation and control systems

狀態：現行標準 最新日期：110/12/24

版本：中文版 價格(新台幣)：475

[預覽](#) [加入購物車](#)

CNS 62443-3-3 X6143-3-3(彩色版)

工業通訊網路 - 網路及系統安全 - 第3-3部：系統安全要求事項及安全等級
Industrial communication networks – Network and system security – Part 3-3:
System security requirements and security levels

狀態：現行標準 最新日期：111/12/15

版本：中文版 價格(新台幣)：385

[預覽](#) [加入購物車](#)

CNS 62443-4-1 X6143-4-1(彩色版)

工業自動化及控制系統之安全性 - 第4-1部：產品開發生命週期之安全要求事項
Security for industrial automation and control systems – Part 4-1: Secure product
development lifecycle requirements

狀態：現行標準 最新日期：110/12/24

版本：中文版 價格(新台幣)：280

[預覽](#) [加入購物車](#)

CNS 62443-4-2 X6143-4-2(彩色版)

工業自動化及控制系統之安全性 - 第4-2部：IACS組件之技術安全要求事項
Security for industrial automation and control systems – Part 4-2: Technical security
requirements for IACS components

狀態：現行標準 最新日期：111/11/03

版本：中文版 價格(新台幣)：415

[預覽](#) [加入購物車](#)

甚麼是 ISA/ IEC 62443?

全球認可

涵蓋技術、流程和人員的全球性方法

針對資產擁有者、系統整合商和產品製造商。

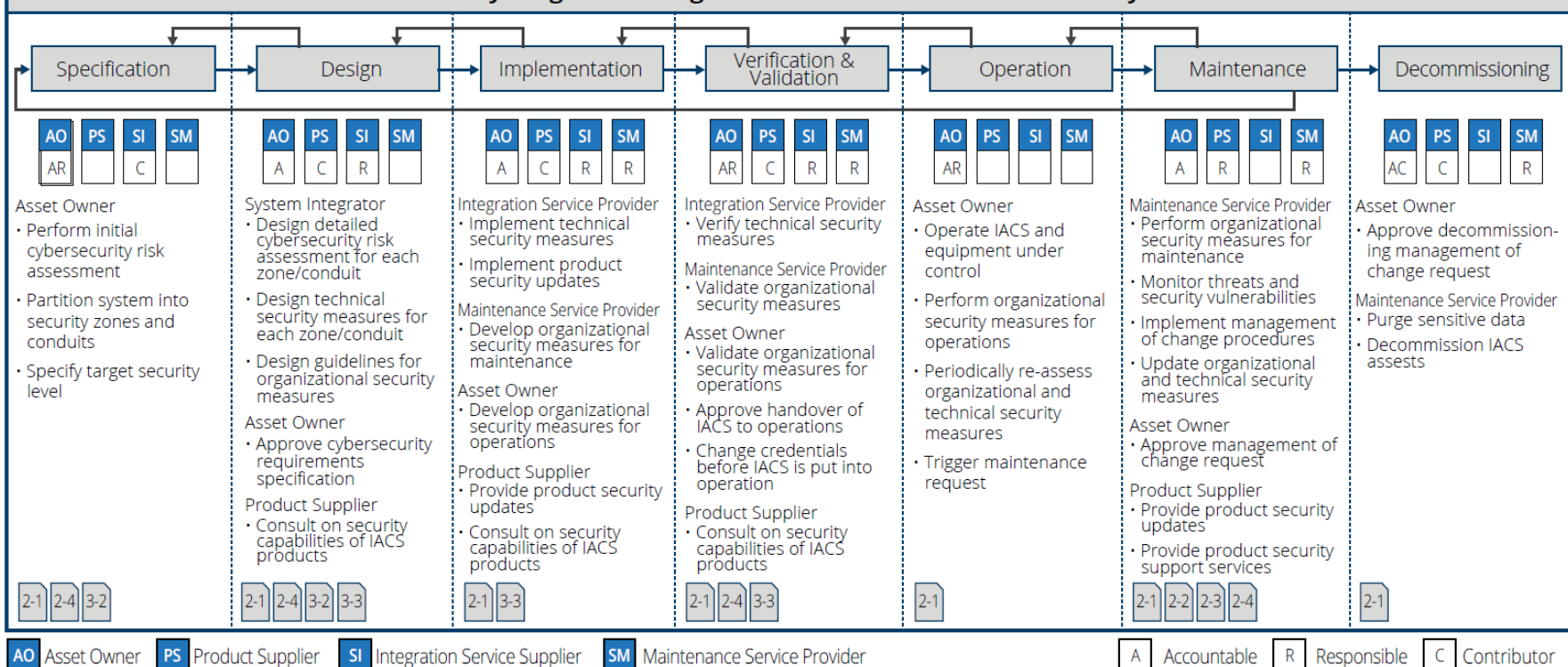
適用於所有工業領域的一套資訊安全標準。

最初設計用於工業控制、發電站、製造業

但也適用於軌道交通、電網、**CTM/BMS**

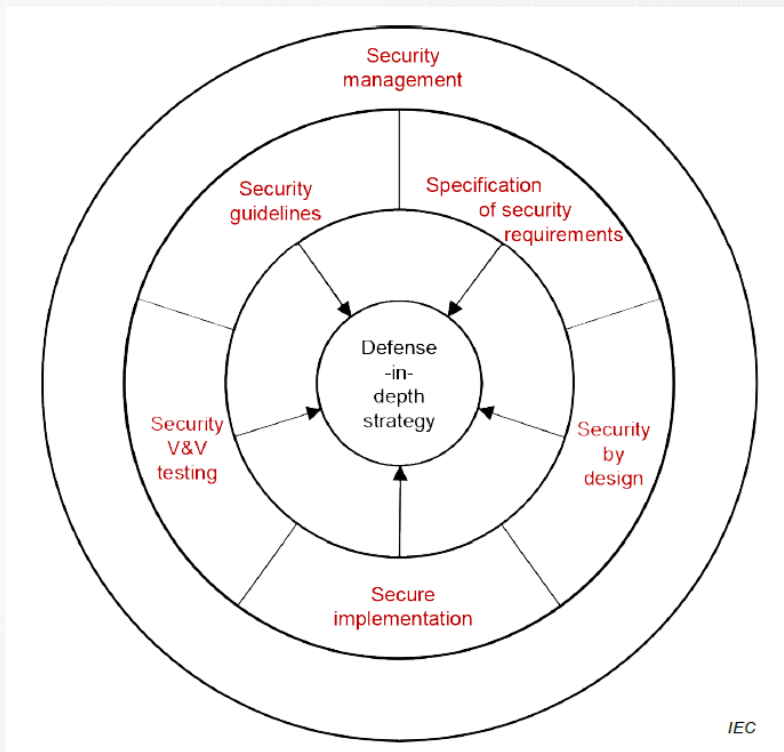


Security Program Throughout the Automation Solution Lifecycle



IEC 62443-4-1 安全產品開發流程

- Security management
- Specification of security requirements
- Secure by design
- Secure implementation
- Security verification and validation testing
- Management of security-related issues
- Security update management
- Security guidelines



IEC 62443-4-1 流程成熟度

Level	CMMI-DEV	IEC 62443-4-1	IEC 62443-4-1 Description
1	Initial	Initial	Product suppliers typically perform product development in an ad-hoc and often undocumented (or not fully documented) manner. As a result, consistency across projects and repeatability of processes may not be possible.
2	Managed	Managed	<p>At this level, the product supplier has the capability to manage the development of a product according to written policies (including objectives). The product supplier also has evidence to show that personnel who will perform the process have the expertise, are trained and/or follow written procedures to perform it.</p> <p>However, at this level, the organization does not have experience developing products to all of the written policies. This would be the case when the organization has updated its procedures to conform to this document, but has not yet put all of the procedures into actual practice, yet.</p> <p>The development discipline reflected by maturity level 2 helps to ensure that development practices are repeatable, even during times of stress. When these practices are in place, their execution will be performed and managed according to their documented plans.</p> <p>NOTE At this level, the CMMI and IEC 62443-4-1 maturity models are fundamentally the same, with the exception that IEC 62443-4-1 recognizes that there may be a significant delay between defining/formalizing a process and executing (practicing) it. Therefore, the execution related aspects of the CMMI-DEV Level 2 are deferred to Level 3.</p>
3	Defined	Defined (Practiced)	<p>The performance of a level 3 product supplier can be shown to be repeatable across the supplier's organization. The processes have been practiced, and evidence exists to demonstrate that this has occurred.</p> <p>NOTE At this level, the CMMI and IEC 62443-4-1 maturity models are fundamentally the same, with the exception that the execution related aspects of the CMMI-DEV level 2 are included here. Therefore, a process at level 3 is a level 2 process that the supplier has practiced for at least one product.</p>
4	Quantitatively Managed	Improving	At this level, Part 4-1 combines CMMI-DEV levels 4 and 5. Using suitable process metrics, product suppliers control the effectiveness and performance of the product and demonstrate continuous improvement in these areas.
5	Optimizing		

常見誤解 #1

“只需動用產品部門資源，便可符合 4-1 流程要求”

Practice 1 - Security Management (SM)

- 確保安全相關活動在產品的整個生命週期中得到充分規劃、文件化和執行。
- 如果在規劃和支援與安全相關的活動時不加注意，那麼由於資源不足、時間不足或流程效率低下，這些活動可能會變得無效。
- 同樣地，如果產品的安全需求與相關的組織流程不匹配，例如組態管理、資訊技術政策和流程以及供應鏈管理，可能會危及安全產品開發生命週期的有效性。

主題

要求

Practice 1 - Security Management (SM)

- SM-1: Development process
- SM-2: Identification of responsibilities
- SM-3: Identification of applicability
- SM-4: Security expertise
- SM-5: Process scoping
- SM-6: File integrity
- SM-7: Development environment security (IT)
- SM-8: Controls for private keys (IT)
- SM-9: Security requirements for externally provided components (Supply Chain)
- SM-10: Custom developed components from third-party (Supply Chain)
- SM-11: Assessing and addressing security-related issues
- SM-12: Process verification
- SM-13: Continuous improvement

常見誤解 #2

“通過 4-1 驗證後，所有產品都須遵守安全產品開發流程”

SM-3: Identification of applicability

- 應採用一個流程來識別適用於 ISA/IEC 62443-4-1 的產品（或部分產品）

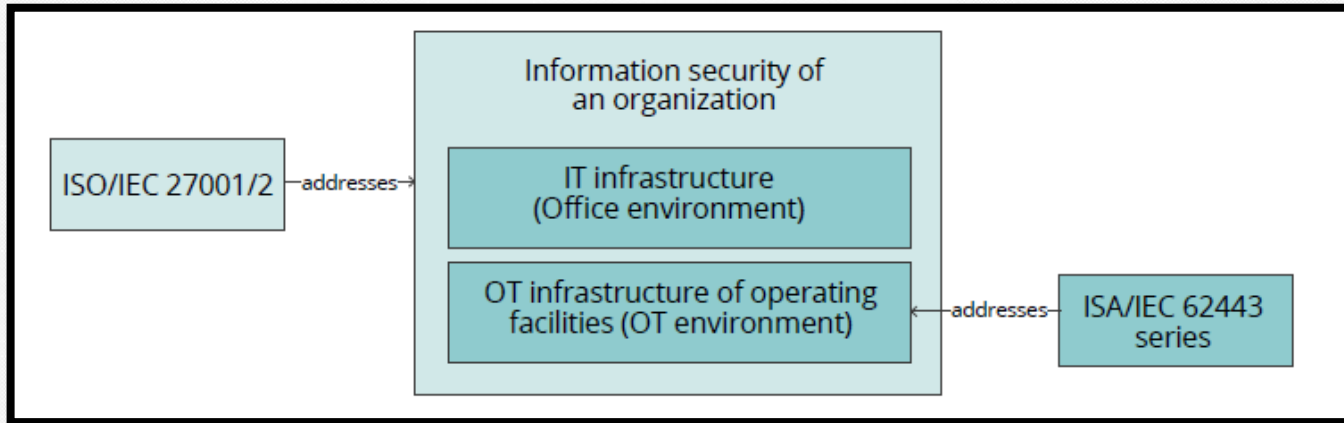
SM-5: Process scoping

- 應採用一個包括通過文件化的安全分析進行理由說明的流程，以識別對選定的產品開發項目適用的本文件的部分。對項目遵循本文件的合規程度進行範圍界定的理由應由具備適當安全專業知識的人員審查和核准。

常見誤解 #3

“公司已經通過 **ISO 27001** 驗證，
因此可以在 **62443** 認證中大量重用其內容”

ISO/IEC 27001/2 and the ISA/IEC 62443



SM-7: Development environment security

- 在產品開發、生產和交付過程中，應採用包含程序性和技術性控制流程來保護產品。這包括在設計、實施、測試和發布過程中保護產品或產品更新（修補程式）。

常見誤解 #4

“產品中的開源軟體不是我們開發的，因此我們不需要對其進行安全評估”

SM-9: Security requirements for externally provided components

- 應採用一個流程來識別和管理產品中使用的所有外部提供組件的安全風險。



Open Source Security Foundation (OpenSSF)

Collaborating to secure the open source ecosystem


[wg-identifying-security-threats](#)

The purpose of the Identifying Security Threats working group is to enable stakeholders to have informed confidence in the security of open source projects. We do this by collecting, curating, and ...

☆ 112  9

[wg-security-tooling](#)

OpenSSF Security Tooling Working Group

☆ 147  15

[wg-best-practices-os-developers](#)

The Best Practices for OSS Developers working group is dedicated to raising awareness and education of secure code best practices for open source developers.

☆ 113  9

[wg-vulnerability-disclosures](#)

The OpenSSF Vulnerability Disclosures Working Group seeks to help improve the overall security of the open source software ecosystem by helping mature and advocate well-managed vulnerability report...

☆ 67  21

[wg-digital-identity-attestation](#)

Our objective is to enable open source maintainers, contributors and end-users to understand and make decisions on the provenance of the code they maintain, produce and use.

☆ 44  5

[wg-securing-critical-projects](#)

Helping allocate resources to secure the critical open source projects we all depend on.

☆ 84  8

SM-10: Custom developed components from third-party

- 應採用一個流程來確保來自第三方供應商的組件的產品開發生命週期流程符合本文件中使用的要求，當它們符合以下標準時：
 - a) 這些組件是為單一供應商特定目的而開發的；
 - b) 這些組件可能對安全性產生影響。

常見誤解 #5

“工控產品要做風險評估”



IEC 62443-3-2

Edition 1.0 2020-06

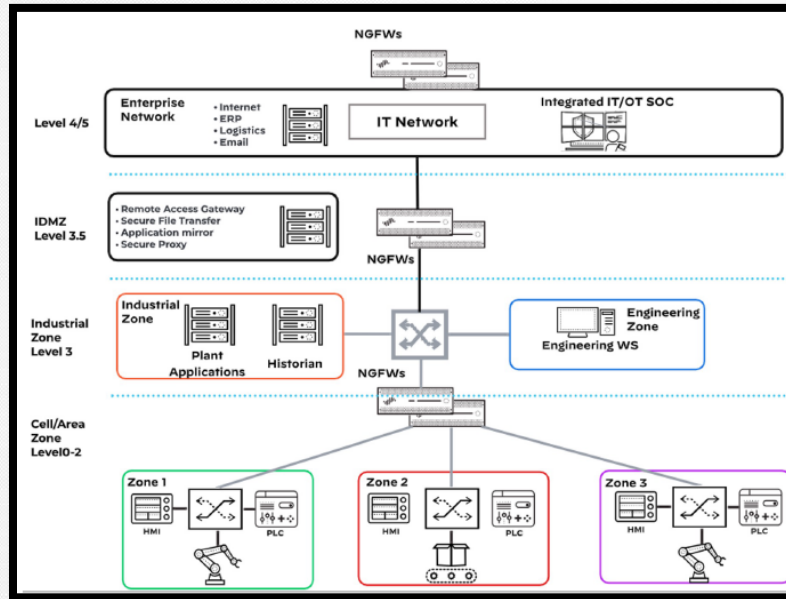
INTERNATIONAL STANDARD



**Security for industrial automation and control systems –
Part 3-2: Security risk assessment for system design**

SR-1: Product security context

- 應該採用一個流程，確保所預期的產品安全情境已經被記錄。



- a) 網路中的位置；
- b) 產品將部署的環境提供的實體或網路安全性；
- c) (從網路角度) 隔離；和
- d) 如果已知，對環境的潛在影響（例如，生命損失，受傷，生產損失等）。

SR-2: Threat model

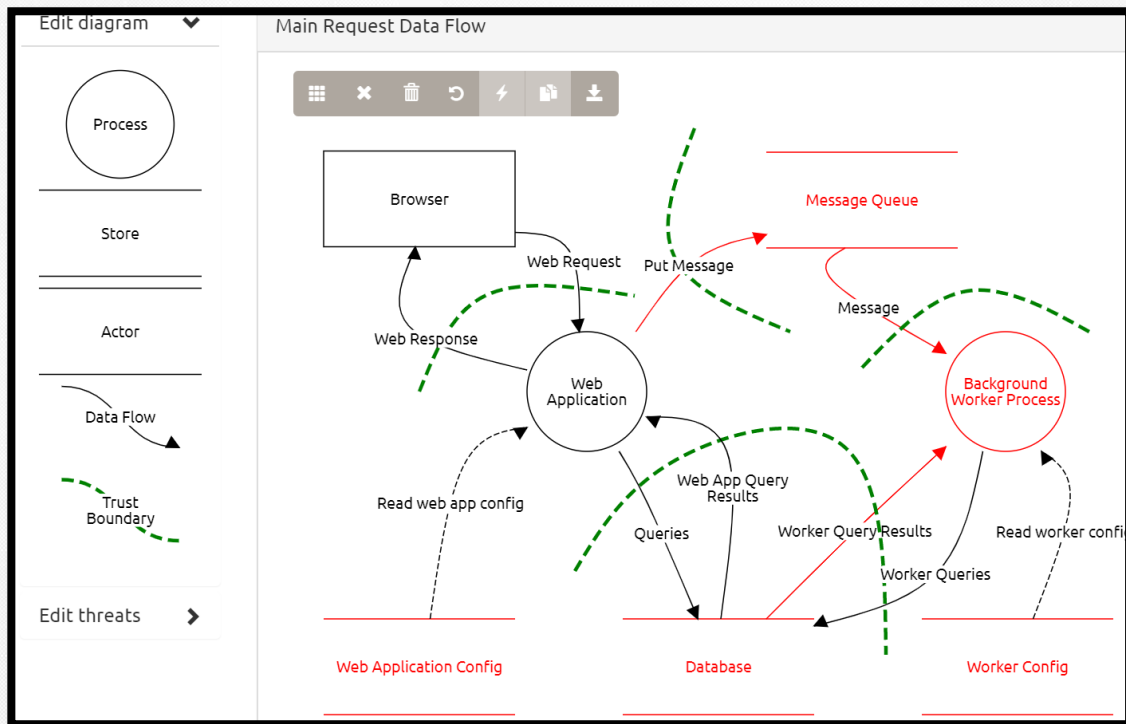
- 應該採用一個流程，確保所有產品都擁有與目前開發範圍相關的威脅模型，該模型具有以下特徵（如適用）：
 - a) 正確的資訊分類在整個系統中流動；
 - b) 信任邊界；
 - c) 流程；
 - d) 資料存儲；
 - e) 與外部實體的互動；
 - f) 產品中實施的內部和外部通訊協定；
 - g) 可供外部訪問的實體介面，包括 **debug** 介面；
 - h) 電路板連接，例如 JTAG 連接 或 **debug** 介面，可能被用來攻擊硬體；
 - i) 潛在的攻擊向量，包括對硬體的攻擊（如適用）；
 - j) 潛在的威脅及其嚴重性，由漏洞評分系統（例如 CVSS）定義；
 - k) 針對每個威脅的緩解措施和/或處理；
 - l) 確定的與安全有關的問題；和
 - m) 連結到應用程式中的驅動程式或第三方應用程式（供應商未開發的程式碼）等外部依賴項。
- 威脅模型應由開發團隊進行審查和驗證，以確保其正確性和理解。
- 威脅模型應定期審查（至少每年一次）對於已發布的產品，並在必要時進行更新，以應對對產品的新威脅的出現，即使設計未更改。

任何在威脅模型中發現的問題都應根據“評估與安全相關的問題”和“解決與安全相關的問題”中定義的方式進行解決。

SR-2: Threat model

Threat Modeling Tool - Data-flow Diagram (DFD)

OWASP-Threat-Dragon



SR-2: Threat model

Threat Modelling Methodologies



Threat source/ viewpoint

Model capability, intent, and targeting for adversarial threats. Find out the actions that the threat agent might conduct.



Threat actions

Model the actions which might be conducted by threat actor. The common method is STRIDE model developed by Microsoft.



Threat activity

Model the activity which is conducted by a series of threat actions to achieve a desired outcome. The common method is attack tree.

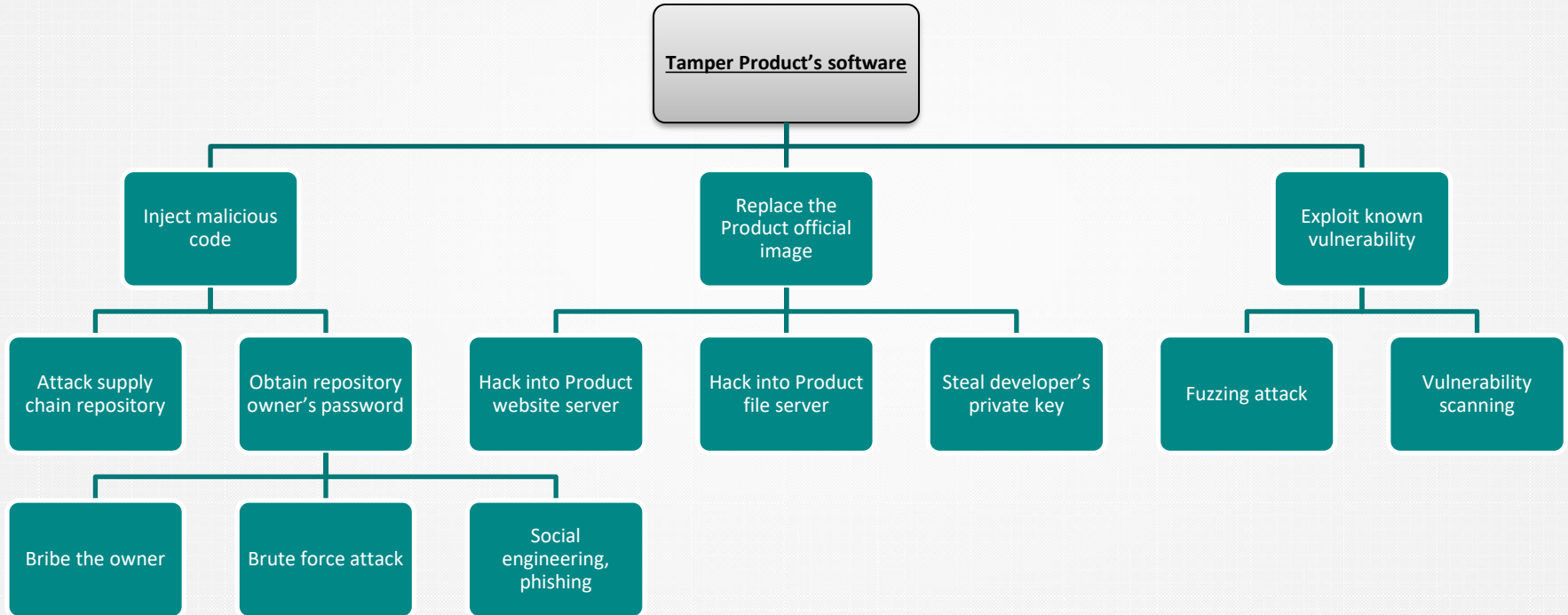


Vulnerability viewpoint

Model the vulnerability within the asset which may exist in the organization. Typically, massive of technical information is essential as indicators

SR-2: Threat model

Attack Tree for Integrity



SR-2: Threat model

Threat Modeling Tool

- Draw.io libraries for threat modelling
 - <https://github.com/michenriksen/drawio-threatmodeling>
- OWASP-Threat-Dragon
 - <https://threatdragon.org/login>
- threatspec
 - <https://threatspec.org/>
- pytm
 - <https://github.com/izar/pytm>
- Microsoft Threat Modelling Tool
 - <https://docs.microsoft.com/en-gb/azure/security/develop/threat-modeling-tool>

常見誤解 #6

“Coding Standard 可以寫一份就好”

SI-2: Secure coding standards

- 實施流程應納入定期審查和更新的安全程式撰寫標準，並至少包括以下內容：
 - a) 避免潛在可利用的實施結構 - 已知存在安全弱點的實施設計模式；
 - b) 避免使用被禁止的功能和程式撰寫結構/設計模式 - 不應使用的軟體功能和設計模式，因為它們已知具有安全弱點；
 - c) 自動化工具的使用和設置（例如，靜態分析工具）；
 - d) 安全程式撰寫實踐；
 - e) 驗證所有跨信任邊界的輸入；
 - f) 錯誤處理。

SI-2: Secure coding standards

SEI CERT C Coding Standard

由 Admin 创建, 最终由 David Svochoda 修改于 十二月 05, 2018

The C rules and recommendations in this wiki are a work in progress and reflect the current thinking of the secure coding community. Because this is a development website, many pages are incomplete or contain errors. As rules and recommendations mature, they are published in report or book form as official releases. These releases are issued as dictated by the needs and interests of the secure software development community.

Create a sign-in account if you want to comment on existing content. If you wish to be more involved and directly edit content on the site, you still need an account, but you'll also need to [request edit privileges](#).

Front Matter

[Introduction](#)

Rules

- [Rule 01. Preprocessor \(PRE\)](#)
- [Rule 02. Declarations and Initialization \(DCL\)](#)
- [Rule 03. Expressions \(EXP\)](#)
- [Rule 04. Integers \(INT\)](#)
- [Rule 05. Floating Point \(FLP\)](#)
- [Rule 06. Arrays \(ARR\)](#)
- [Rule 07. Characters and Strings \(STR\)](#)
- [Rule 08. Memory Management \(MEM\)](#)
- [Rule 09. Input Output \(FIO\)](#)
- [Rule 10. Environment \(ENV\)](#)
- [Rule 11. Signals \(SIG\)](#)
- [Rule 12. Error Handling \(ERR\)](#)
- [Rule 13. Application Programming Interfaces \(API\)](#)
- [Rule 14. Concurrency \(CON\)](#)
- [Rule 48. Miscellaneous \(MSC\)](#)

Recommendations

- [Rec. 01. Preprocessor \(PRE\)](#)
- [Rec. 02. Declarations and Initialization \(DCL\)](#)
- [Rec. 03. Expressions \(EXP\)](#)
- [Rec. 04. Integers \(INT\)](#)
- [Rec. 05. Floating Point \(FLP\)](#)
- [Rec. 06. Arrays \(ARR\)](#)
- [Rec. 07. Characters and Strings \(STR\)](#)
- [Rec. 08. Memory Management \(MEM\)](#)
- [Rec. 09. Input Output \(FIO\)](#)
- [Rec. 10. Environment \(ENV\)](#)
- [Rec. 11. Signals \(SIG\)](#)
- [Rec. 12. Error Handling \(ERR\)](#)
- [Rec. 13. Application Programming Interfaces \(API\)](#)
- [Rec. 14. Concurrency \(CON\)](#)
- [Rec. 48. Miscellaneous \(MSC\)](#)

CERT manifest files

As of 9/28/2018, the [CERT manifest files](#) are now available for use by static analysis tool developers to test their coverage of (some of the) CERT Secure Coding Rules for C, using many of 61,387 test cases in the Juliet test suite v1.2.

Secure C Coding Books and Downloads



The CERT C Coding Standard, 2016 Edition provides rules to help programmers ensure that their code complies with the new C11 standard and earlier standards, including C99. It is downloadable as a PDF. ([errata](#))



[Secure Coding in C and C++](#) identifies the root causes of today's most widespread software vulnerabilities, shows how they can be exploited, reviews the potential consequences, and presents secure alternatives.

SI-2: Secure coding standards

The CWE Top 25

Below is a brief listing of the weaknesses in the 2020 CWE Top 25, including the overall score of each.

Rank	ID	Name	Score
[1]	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	46.82
[2]	CWE-787	Out-of-bounds Write	46.17
[3]	CWE-20	Improper Input Validation	33.47
[4]	CWE-125	Out-of-bounds Read	26.50
[5]	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	23.73
[6]	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20.69
[7]	CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	19.16
[8]	CWE-416	Use After Free	18.87
[9]	CWE-352	Cross-Site Request Forgery (CSRF)	17.29
[10]	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16.44

常見誤解 #7

“使用弱點掃描工具已足夠”

SVV-3: Vulnerability testing

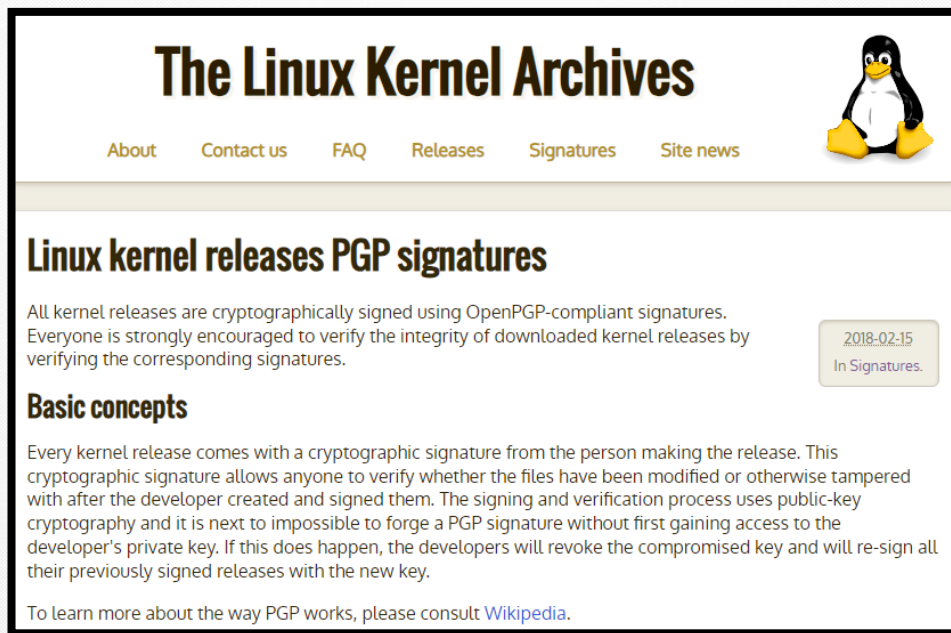
- 應採用流程進行測試，重點是識別和描述產品中潛在的安全漏洞。已知漏洞測試應至少基於建立的、行業公認的、公開的已知漏洞來源的最新內容。測試應包括：
 - a) 濫用案例或意外輸入測試，重點是發現安全問題。這應包括手動或自動的濫用案例測試，以及對所有外部介面和協定進行特殊類型的濫用案例測試，只要有相應的工具。示例包括模糊測試、網路流量負載測試和容量測試；
 - b) 攻擊面分析，以確定系統的所有進出口介面，常見漏洞包括但不限於弱ACL、外露介面和以提升權限運行的服務；
 - c) 黑盒已知漏洞掃描，重點是在產品硬體、主機或軟體組件中檢測已知的漏洞。例如，這可能是基於網路的已知漏洞掃描；
 - d) 對於編譯的軟體，應對供應商交付的所有二進制可執行文件進行軟體組成分析，包括嵌入式韌體。該分析應至少檢測以下類型的問題：
 - 產品軟體組件中的已知漏洞；
 - 鏈接到有漏洞的函式庫；
 - 安全規則違規；以及
 - 可導致漏洞的編譯器設定；
 - e) 動態運行時資源管理測試，檢測在靜態程式碼分析下不可見的缺陷，包括但不限於由於未能釋放運行時 handler、記憶體洩漏和未經身份驗證地存取共享記憶體而導致的服務拒絕條件。如果有這樣的工具，則應應用此測試。

常見誤解 #8

“更新時，提供更新檔就好”

SUM-4: Security update delivery

- 應採用一個流程來確保所有支援的產品和產品版本的安全更新以一種便於驗證安全修補程式**真實性**的方式提供給產品使用者。



Questions?



IEC 62443-4-2

Edition 1.0 2019-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Security for industrial automation and control systems –
Part 4-2: Technical security requirements for IACS components**

**Sécurité des systèmes d'automatisation et de commande industrielles –
Partie 4-2: Exigences de sécurité technique des composants IACS**

常見誤解 #1

“產品只需要看 4-1 & 4-2 就好”

4-2 中, 明確指出需要參考 ISA/IEC 62443-3-3 的條文

Requirement	Description	Security Level
CR 1.1 – Human user identification and authentication	Components shall provide the capability to identify and authenticate all human users according to IEC 62443-3-3 SR 1.1 on all interfaces capable of human user access. This capability shall enforce such identification and authentication on all interfaces that provide human user access to the component to support segregation of duties and least privilege in accordance with applicable security policies and procedures. This capability may be provided locally by the component or by integration into a system level identification and authentication system.	1,2,3,4
CR 1.2 – Software process and device identification and authentication	Components shall provide the capability to identify itself and authenticate to any other component (software application, embedded devices, host devices and network devices), according to IEC 62443-3-3 SR1.2 .	2,3,4
...
CR 4.1 – Information confidentiality	Components shall a) provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported; and b) support the protection of the confidentiality of information in transit as defined in IEC 62443-3-3 SR 4.1 .	1,2,3,4
CR 7.8 – Control system component inventory	Components shall provide the capability to support a control system component inventory according to IEC 62443-3-3 SR 7.8 .	2,3,4

常見誤解 #2

“Embedded Device 是嵌入式設備”

ISA/ IEC 62443-4-2 Component Type

Host device	Embedded device	Network device	Software application
<ul style="list-style-type: none">● general purpose device running an operating system (for example Microsoft Windows OS or Linux) capable of hosting one or more software applications, data stores or functions from one or more suppliers	<ul style="list-style-type: none">● special purpose device designed to directly monitor or control an industrial process EXAMPLE PLCs, wired or wireless field sensor devices, wired or wireless field actuator devices, safety instrumented system (SIS) controllers, distributed control system (DCS) controllers.	<ul style="list-style-type: none">● device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process	<ul style="list-style-type: none">● one or more software programs and their dependencies that are used to interface with the process or the control system itself (for example, configuration software and historian)

ISA/ IEC 62443-4-2 Component Type

Host device	Embedded device	Network device	Software application
<ul style="list-style-type: none">● general purpose device running an operating system (for example Microsoft Windows OS or Linux) capable of hosting one or more software applications, data stores or functions from one or more suppliers	<ul style="list-style-type: none">● special purpose device designed to directly monitor or control an industrial process EXAMPLE PLCs, wired or wireless field sensor devices, wired or wireless field actuator devices, safety instrumented system (SIS) controllers, distributed control system (DCS) controllers.	<ul style="list-style-type: none">● device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process	<ul style="list-style-type: none">● one or more software programs and their dependencies that are used to interface with the process or the control system itself (for example, configuration software and historian)

常見誤解 #3

“Essential Function 是必要功能”

CCSC 1: Support of **essential functions**

- The components of the system shall adhere to specific constraints as described in IEC 62443-3-3:2013, Clause 4.

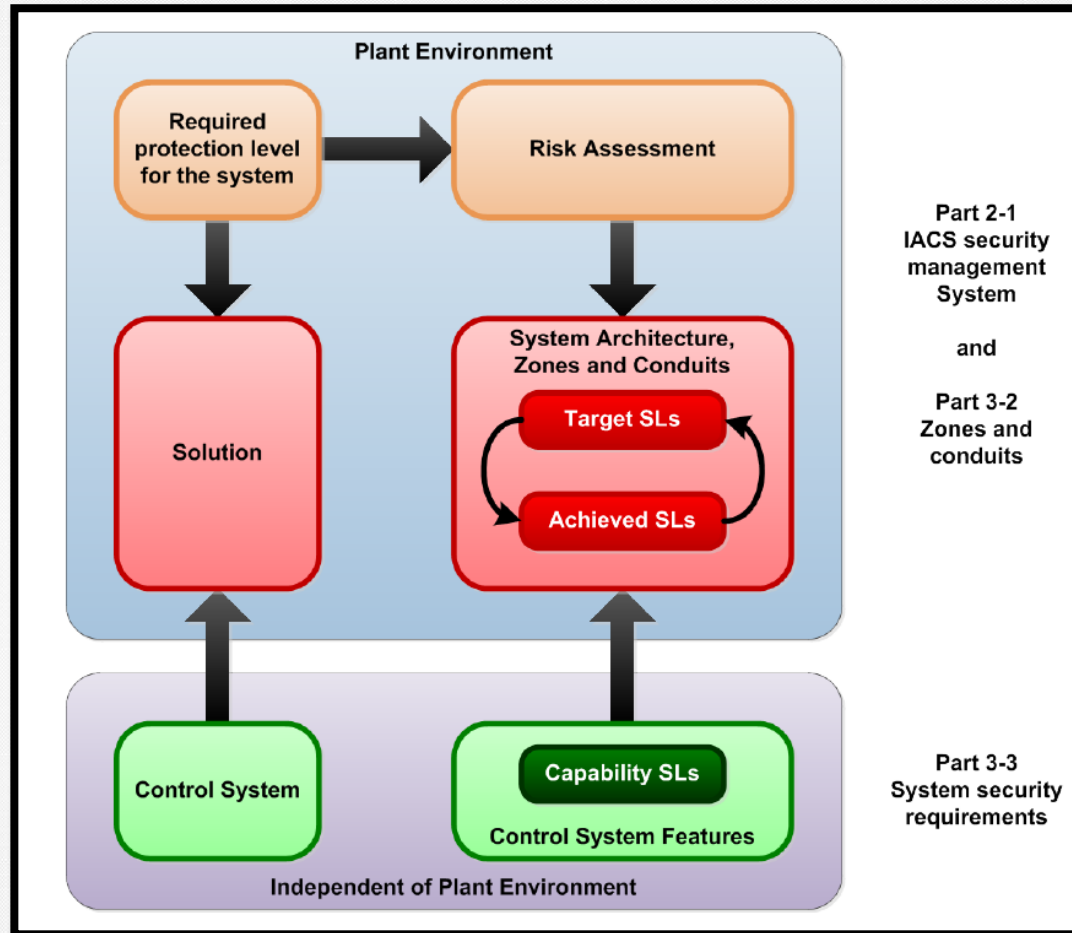
Definition of Essential Function

- function or capability that is required to maintain **health, safety, the environment (HSE)** and **availability for the equipment under control**.
- Note 1 to entry: Essential functions include, but are not limited to, the safety instrumented function (SIF), the control function and the ability of the operator to view and manipulate the equipment under control. The loss of essential functions is commonly termed loss of protection, loss of control and loss of view respectively. In some industries additional functions such as history may be considered essential.

常見誤解 #4

“Security Level 由產品製造商自行決定”

Security Level	Description	Threat Actor	Examples of Actors
SL 1	Protection against casual or coincidental violation	Insider and/or External	<ul style="list-style-type: none"> careless or disgruntled employees or contractors intruders with low skills and motivation
SL 2	Protection against intentional violation using simple means with low resources, generic skills, and low motivation		
SL 3	Protection against intentional violation using sophisticated means with moderate resources, system-specific skills, and average motivation	External “professionals”	<ul style="list-style-type: none"> cybercriminals industrial espionage state-sponsored malicious actors
SL 4	Protection against intentional violation using sophisticated means with extended resources, system-specific skills, and high motivation		



常見誤解 #5

“Mobile Code 跟行動裝置有關”

Definition of Mobile Code

- program transferred between assets that can be executed without explicit installation by the recipient
- EXAMPLE JavaScript, VBScript, Java applets, ActiveX controls, Flash animations, Shockwave movies, and Microsoft Office macros.

HDR 2.4 – Mobile code

Requirement	Description	Security Level
HDR 2.4 – Mobile code	<p>當主機裝置使用行動碼技術時，該裝置應具備強制執行針對行動碼技術使用的安全政策的能力。該安全政策至少應允許對於主機裝置上每種行動碼技術進行以下動作：</p> <ul style="list-style-type: none">a) 控制行動碼的執行；b) 控制哪些使用者（人類、軟體程式或裝置）被允許將移動代碼上傳至主機裝置；以及c) 基於對行動碼的完整性檢查，在程式執行之前控制程式的執行。	1,2,3,4
HDR 2.4 RE 1 – Mobile code authenticity check	<p>主機裝置應提供強制執行安全政策的能力，該政策允許裝置在程式執行之前，根據對行動碼進行的真實性檢查結果，控制行動碼的執行。</p>	2,3,4

常見誤解 #6

“Input validation 只跟操作介面輸入有關”

CR 3.5 – Input validation

Requirement	Description	Security Level
CR 3.5 – Input validation	Components shall validate the syntax, length and content of any input data that is used as an industrial process control input or input via external interfaces that directly impacts the action of the component.	1,2,3,4

CR 3.5 – Input validation

Requirement	Description	Security Level
CR 3.5 – Input validation	Components shall validate the syntax, length and content of any input data that is used as an industrial process control input or input via external interfaces that directly impacts the action of the component.	1,2,3,4

常見誤解 #7

“軟體完整性/ 真實性只要開機時檢查就好”

CR 3.4 – Software and information integrity

Requirement	Description	Security Level
CR 3.4 – Software and information integrity	組件應具備執行或支援對軟體、設定和其他資訊進行完整性檢查的能力，包括記錄和報告這些檢查的結果，或能整合到能夠執行或支援完整性檢查的系統中。	1,2,3,4
CR 3.4 RE 1 – Authenticity of software and information	此外，組件也應具備執行或支援對軟體、設定和其他資訊進行真實性檢查的能力，包括記錄和報告這些檢查的結果，或能整合到能夠執行或支援真實性檢查的系統中。	2,3,4
CR 3.4 RE 2 – Automated notification about integrity violations	若組件負責執行完整性檢查，則應能在發現未授權更改的嘗試時，自動向可設定的對象發出通知。	3,4

常見誤解 #8

“DoS 類型自行挑選即可”

CR 7.1 – Denial of service protection

Requirement	Description	Security Level
CR 7.1 – Denial of service protection	組件應具備在因DoS（拒絕服務）事件導致降級模式運作時維持 essential function 的能力。	1,2,3,4
CR 7.1 RE 1 – Manage communication load from component	組件應提供緩解 DoS 事件的資訊和/或訊息泛洪類型影響的能力。	2,3,4

SR-2: Threat model

- 應該採用一個流程，確保所有產品都擁有與目前開發範圍相關的威脅模型，該模型具有以下特徵（如適用）：
 - a) 正確的資訊分類在整個系統中流動；
 - b) 信任邊界；
 - c) 流程；
 - d) 資料存儲；
 - e) 與外部實體的互動；
 - f) 產品中實施的內部和外部通訊協定；
 - g) 可供外部訪問的實體介面，包括 **debug** 介面；
 - h) 電路板連接，例如 JTAG 連接 或 **debug** 介面，可能被用來攻擊硬體；
 - i) 潛在的攻擊向量，包括對硬體的攻擊（如適用）；
 - j) 潛在的威脅及其嚴重性，由漏洞評分系統（例如 **CVSS**）定義；
 - k) 針對每個威脅的緩解措施和/或處理；
 - l) 確定的與安全有關的問題；和
 - m) 連結到應用程式中的驅動程式或第三方應用程式（供應商未開發的程式碼）等外部依賴項。
- 威脅模型應由開發團隊進行審查和驗證，以確保其正確性和理解。
- 威脅模型應定期審查（至少每年一次）對於已發布的產品，並在必要時進行更新，以應對對產品的新威脅的出現，即使設計未更改。

任何在威脅模型中發現的問題都應根據“評估與安全相關的問題”和“解決與安全相關的問題”中定義的方式進行解決。

常見誤解 #9

“每個條文是獨立存在的”

CR 7.8 – Control system component inventory

Requirement	Description	Security Level
CR 7.8 – Control system component inventory	Components shall provide the capability to support a control system component inventory according to IEC 62443-3-3 SR 7.8.	2,3,4



重新確認先前的條文

Requirement	Security Level
CR 1.2 – Software process and device identification and authentication	2,3,4
CR 1.3 – Account management	1,2,3,4
CR 1.14 – Strength of symmetric key-based authentication	2,3,4
...	...
CR 4.1 – Information confidentiality	1,2,3,4
...	...

常見誤解 #10

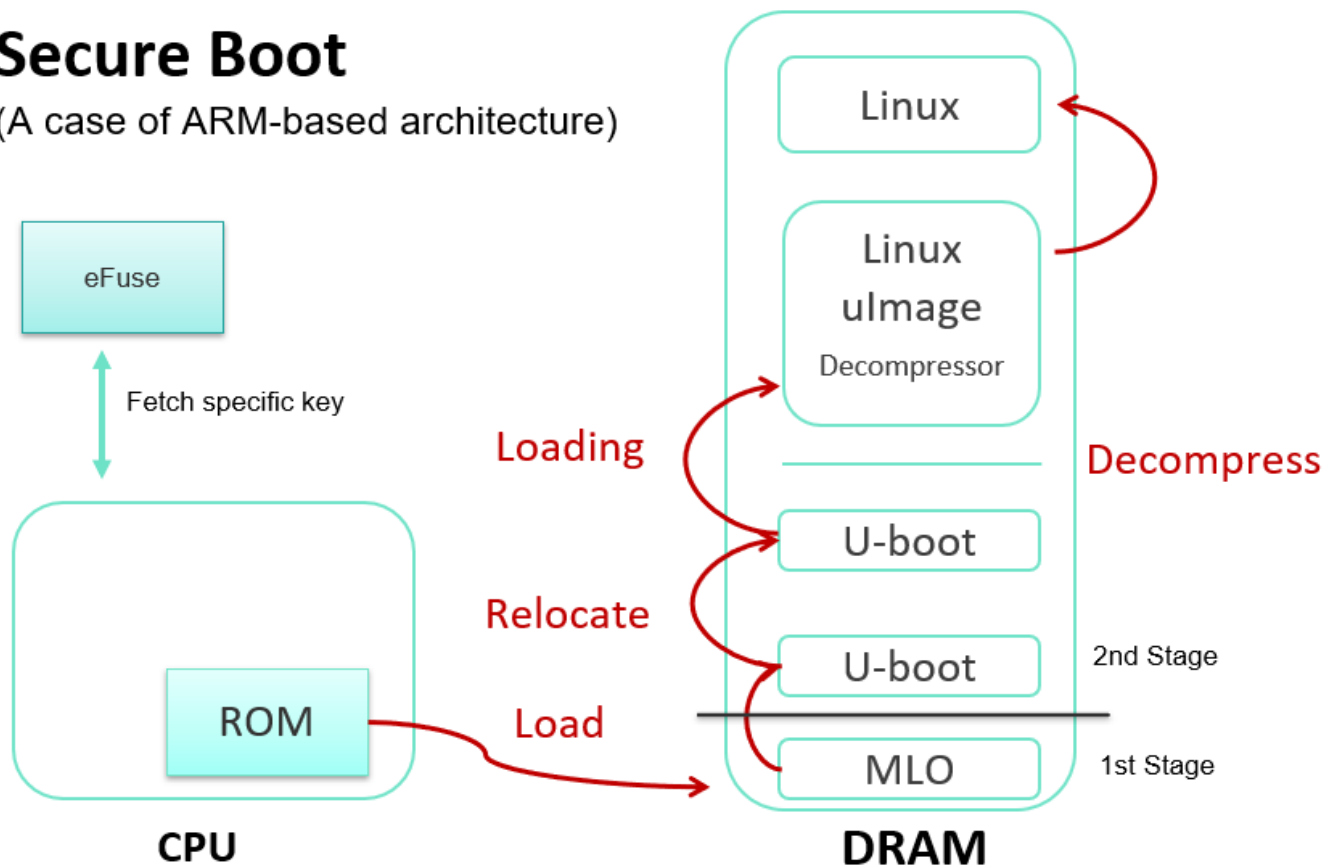
“現有產品透過更新軟韌體便能達到 4-2 合規要求”

硬體相關條文

Requirement	Security Level
CR 1.5 (1) Hardware security for authenticators	3,4
CR 1.14 (1) Hardware security for symmetric key-based authentication	3,4
CR 3.9 (1) Audit records on write-once media	4
{EDR,HDR,NDR} 3.12 – Provisioning product supplier roots of trust	2,3,4
{EDR,HDR,NDR} 3.14 (1) Authenticity of the boot process	2,3,4

Secure Boot

(A case of ARM-based architecture)



Questions?

True or False

“通過 4-2 認可的產品很安全”

True or False

“作為系統整合商，選擇擁有 4-2 證書的產品即可”

ICSA-500

ISA Security Compliance Institute — IIoT Component Security Assurance — Selected commonly accepted security practices

Version 1.1

January 2023

4.1.1 Practices

IIoT PR 4.1.1-1 Cryptographic techniques

Cryptographic algorithms, including key lengths selected and random number generation methods used, conform to ISO/IEC 19790, or conform to an approved national or regional modification to Annex C of ISO/IEC 19790 (noting that such modifications are permitted by ISO/IEC 19790). There should be no reliance on proprietary or modified cryptographic algorithms. The following are examples of documents that provide conforming methods:

- For the United States, methods referenced in [FIPS-140-3 Modules](#) fall under this practice. FIPS-140-3 references [revision 1 "CMVP Validation Authority Updates to ISO/IEC 19790" in NIST SP 800-131A revision 2 "Transitioning the Use of Cryptographic Algorithms"](#)
- For recommendations developed for the European Union, see [Parameters Report. 2014 Recommendations](#)
- From Germany Federal Office for Information Security, [Recommendations and Key Lengths" Version: 2022-1](#)

ICSA-311 FSA-CR 3.4 Software and information integrity *Components shall provide the capability to perform or support integrity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support integrity checks.*

4.5.3 External references

Example references that support above requirements as commonly accepted practices:

[TCG Guidance for Securing Industrial Control Systems Using TCG Technology](#) states in 4.2: "Secure and Measured Boot can be extended to run-time software through mechanisms such as the Linux Integrity Measurement Architecture."

Example references regarding implementation of these practices:

Linux Integrity Measurement Architecture (IMA) and Advanced Intrusion Detection Environment (AIDE) are examples of utilities that can be used to support the above practices.

Linux IMA is a kernel solution, described in the first four references below. Linux IMA natively provides automatic triggering of integrity checking for files as they are used. AIDE is a user space solution, described in the last reference. AIDE natively provides integrity checking triggered on-demand.

[An Overview of The Linux Integrity Subsystem](#)

<https://www.kernel.org/doc/html/latest/security/IMA-templates.html>

<https://www.redhat.com/ja/blog/how-use-linux-kernels-integrity-measurement-architecture>

[TCG Guidance for Securing Industrial Control Systems Using TCG Technology](#) discusses IMA in 6.12.1

<https://aide.github.io/>



IEC/TR 62443-3-1

Edition 1.0 2009-07

TECHNICAL REPORT



**Industrial communication networks – Network and system security –
Part 3 1: Security technologies for industrial automation and control systems**

Thank you