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

ISA/ IEC 62443-4-2:2019

Security Capability Training

by SZ Lin (林上智)

FOR ADLINK USE ONLY

BUREAU VERITAS
CONSUMER **PRODUCTS** SERVICES

SUPPLY CHAIN TRUST SOLUTIONS
Testing • Inspections • Audits • Certification • Advisory • Actionable Insights

Syllabus

課程名稱：深入探索 ISA/IEC 62443-4-2：工業自動化與控制系統產品安全技術要求
課程概述：這個課程是專為深入剖析 ISA/IEC 62443-4-2 標準而設計，該標準是工業自動化和控制系統產品安全的關鍵指南。我們將逐項解析標準中的技術要求，結合案例研究和詳細解說，幫助學員有效評估和提高產品的安全水平。

課程內容：
- 深入解析標準要求：詳細探討 ISA/IEC 62443-4-2 的技術要求，包括身份驗證、存取控制、通訊安全和保證產品完整性的措施。
- 實際案例分析：分享實際案例，深入了解實務中的技術挑戰和解決方法。
- 業界最佳實踐探討：提供業界實際應用這些標準的案例，分享實用的最佳實踐方法。
- 實務問題探討：討論實際應用中常見的問題及其解決策略。
- 互動式問答環節：透過問答互動，加強對標準的理解和應用能力。

For ADLINK USE ONLY

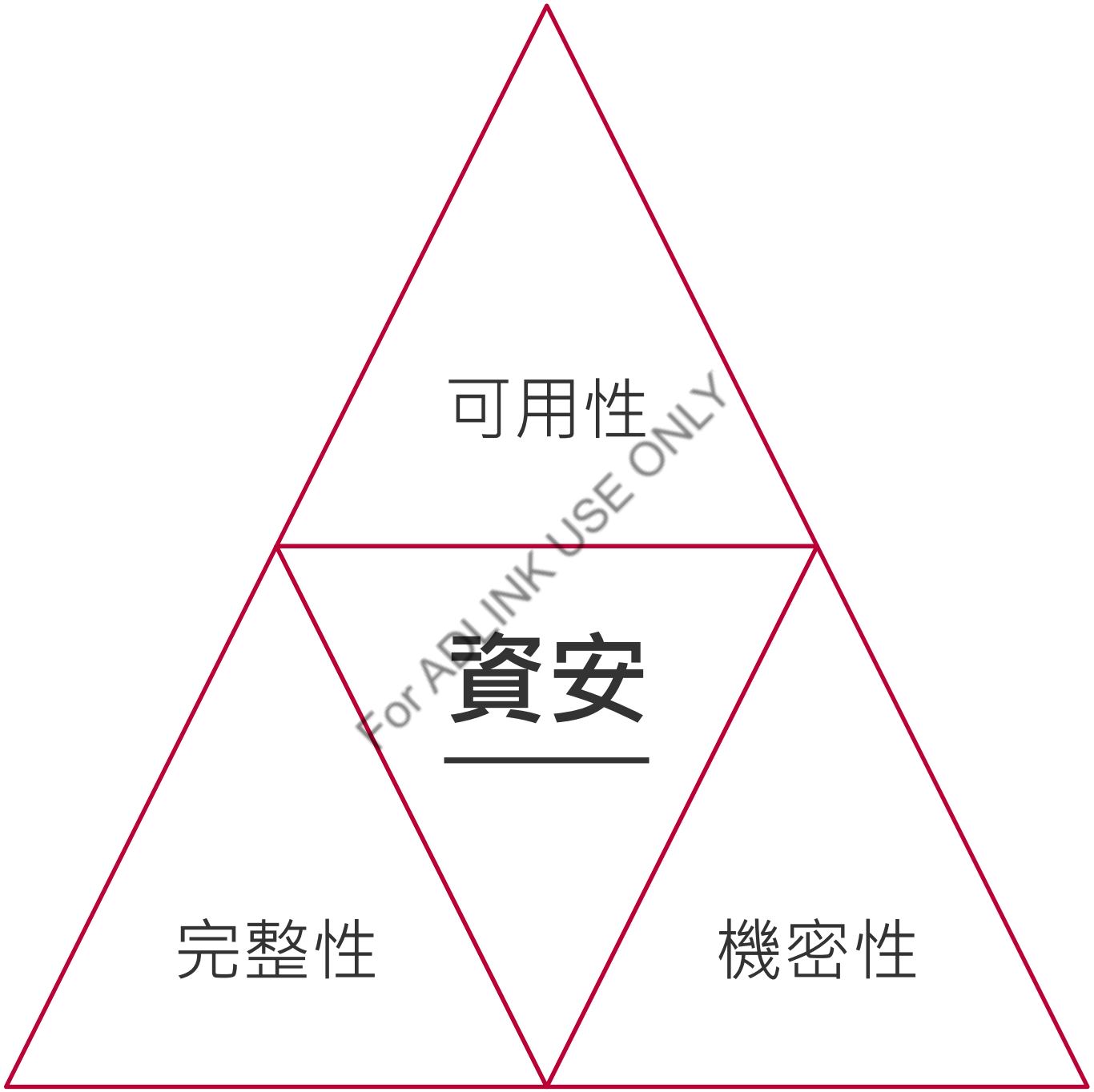
適合參與者： 此課程特別適合那些需要深入理解並實際應用 ISA/IEC 62443-4-2 標準的工業自動化專業人員，如資安工程師、系統架構師、以及軟硬體研發人員。

課程時長：
- **3 小時**

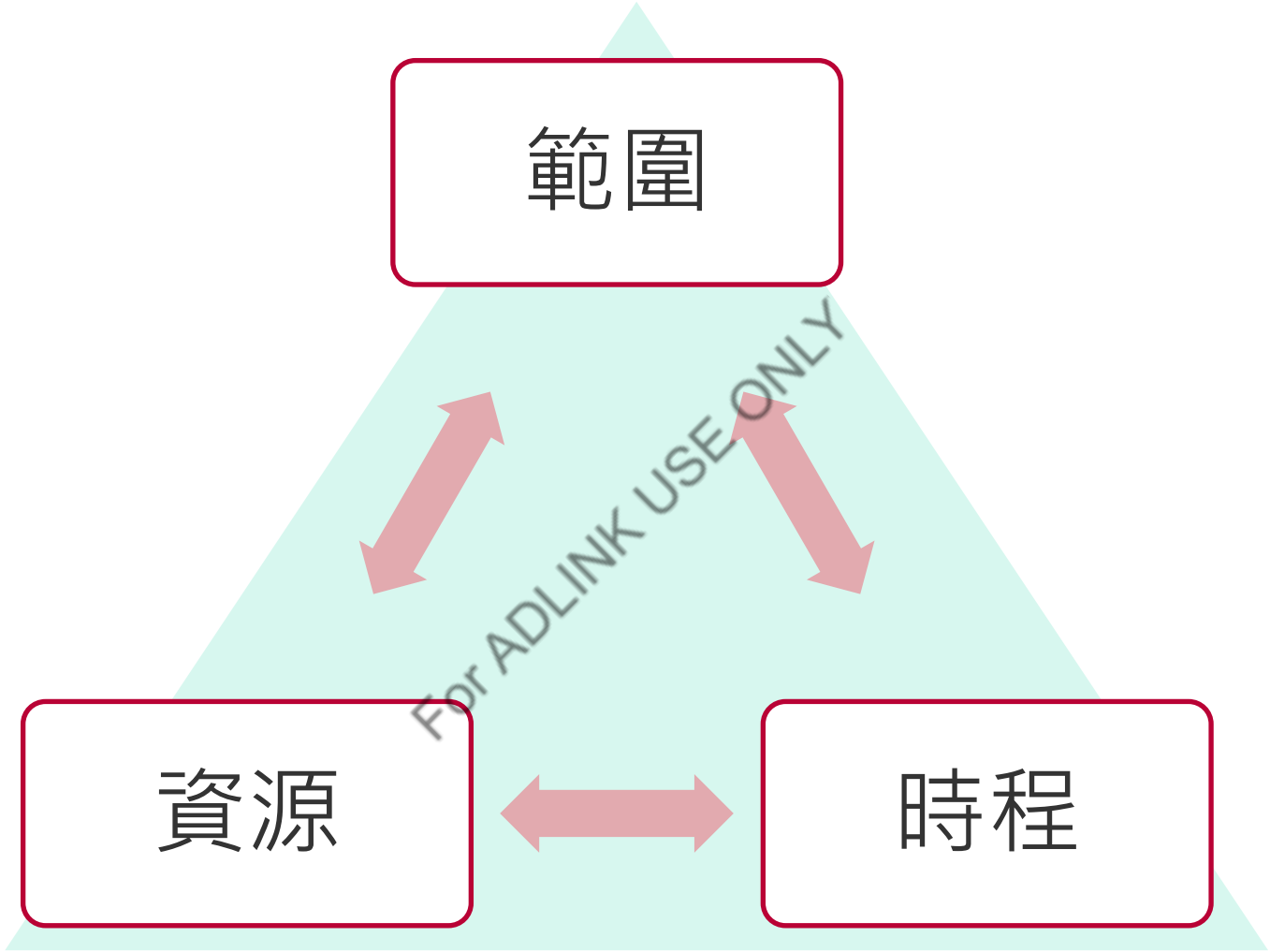
教學方式：
課程結合深入的理論教學、實際案例分析、互動問答和專家指導，旨在為學員提供一個全方位的學習體驗。

基礎觀念

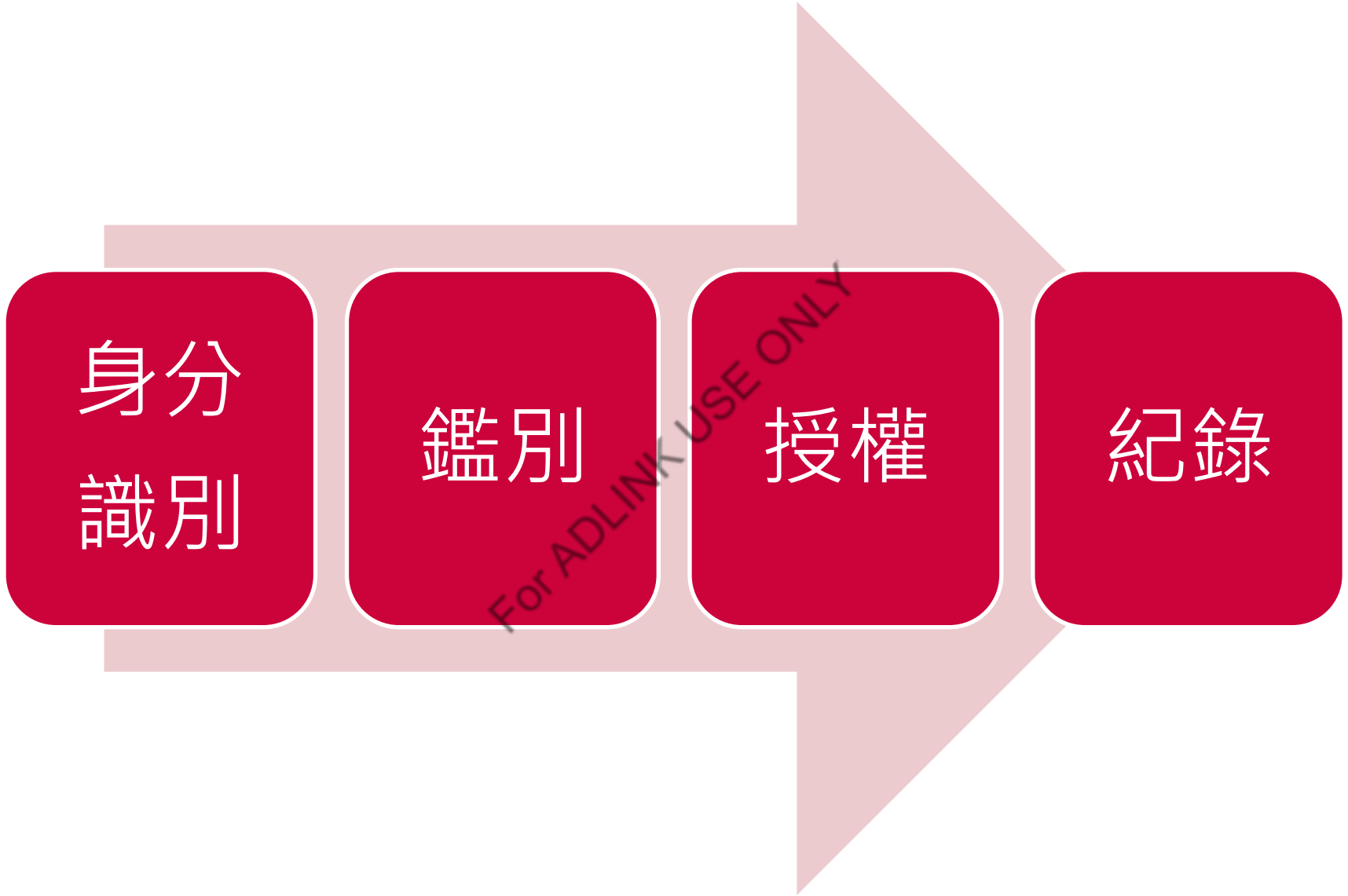
For ADLINK USE ONLY



For ADLINK USE ONLY



For ADLINK USE ONLY



For ADLINK USE ONLY

鑑別因子

- 你有甚麼 - Ownership based authentication.
- 你是甚麼 - Characteristic based authentication.
- 你知道甚麼 - Knowledge based authentication
- 你做甚麼 - Something you do
- 你在哪裡 - Somewhere you are

For ADLINK USE ONLY

兩因子鑑別 (Two-factor authentication)
跟
兩階段鑑別 (Two-step authentication)

For ONLINE USE ONLY

為什麼要做資安

For ADLINK USE ONLY

What is Risk?

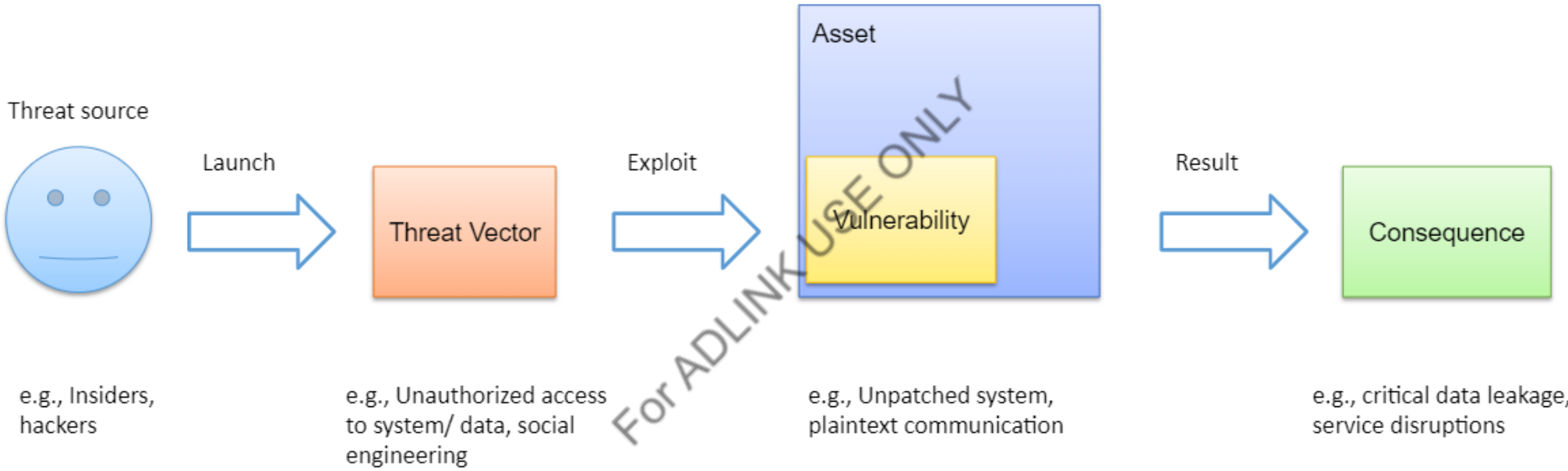
For ADLINK USE ONLY

Risk

‘risk’ means the combination of the probability of occurrence of harm and the severity of that harm

For ALL INHOUSE ONLY

Cybersecurity Risk



For ADLINK USE ONLY

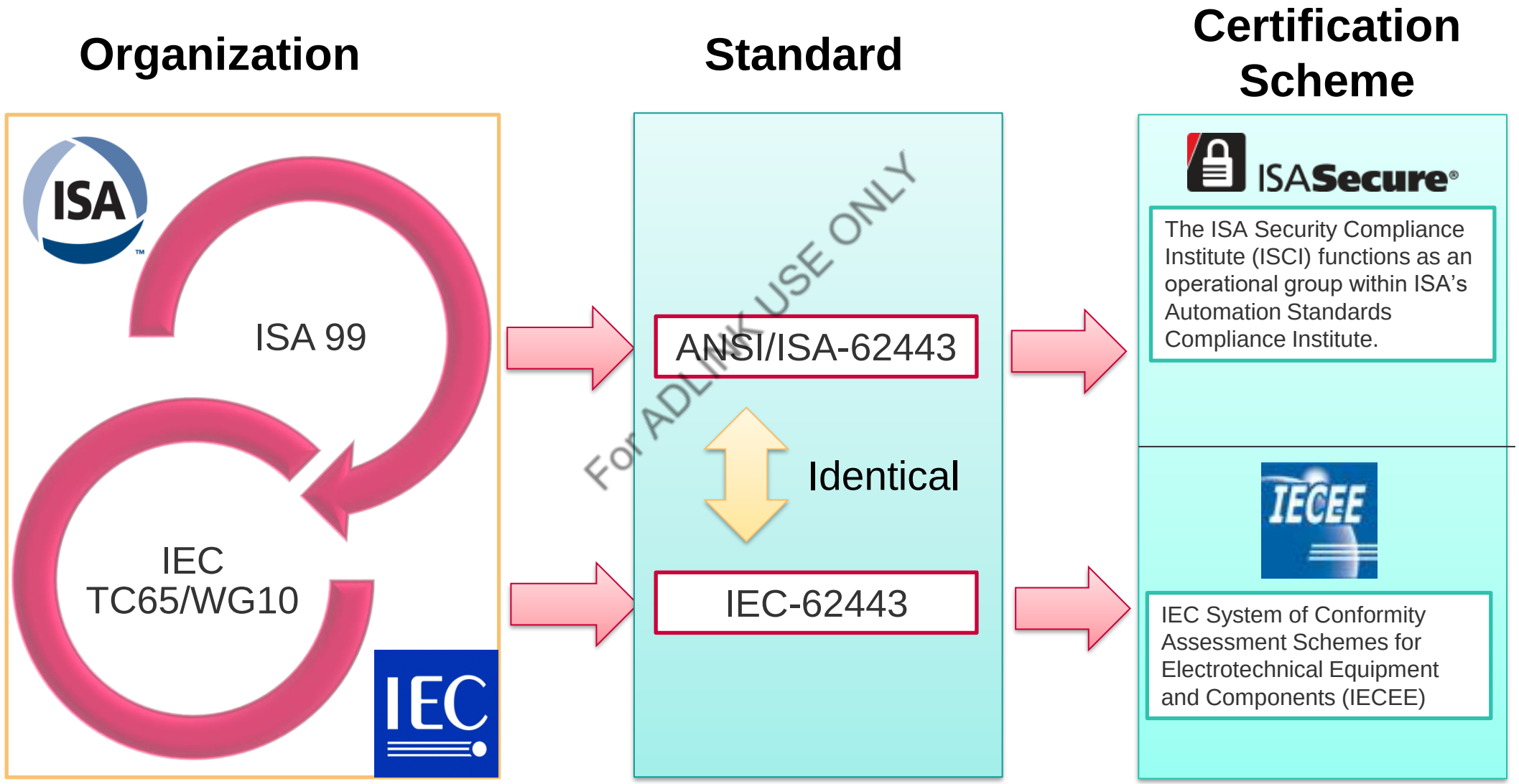
Risk = Threat X Vulnerability X Consequence

For ADLINK USE ONLY

ISA/ IEC 62443

Security for industrial automation and control systems

STANDARDS DEVELOPMENT ORGANIZATION COLLABORATION



ISA/IEC 62443 CERTIFICATION SCHEME

Certified Site (SDLA)
ISASecure
ISA/IEC 62443-4-1

Certified System (SSA)
ISASecure
ISA/IEC 62443-4-1
ISA/IEC 62443-3-3

Certified Component (CSA)
ISASecure
ISA/IEC 62443-4-1
ISA/IEC 62443-4-2

Certified Component (ICSA)
ISASecure
ISA/IEC 62443-4-1
ISA/IEC 62443-4-2

Part	Type	Title	Date
General			
1-1	TS	Terminology, Concepts, and Models	2007
1-2	TR	Master glossary of terms and abbreviations	
1-3		System cybersecurity conformance metrics	
1-4		IACS security lifecycle and use cases	
Policies & Procedures			
2-1	IS	Establishing an IACS security program	2009
2-2		IACS security program ratings	
2-3	TR	Patch management in the IACS environment	2015
2-4	IS	Security program requirements for IACS service providers	2018
2-5	TR	Implementation guidance for IACS asset owners	
System			
3-1	TR	Security technologies for IACS	
3-2	IS	Security risk assessment for system design	2020
3-3	IS	System security requirements and security levels	2013
Component			
4-1	IS	Product security development life-cycle requirements	2018
4-2	IS	Technical security requirements for IACS components	2019

For ADLINK USE ONLY

IECEE

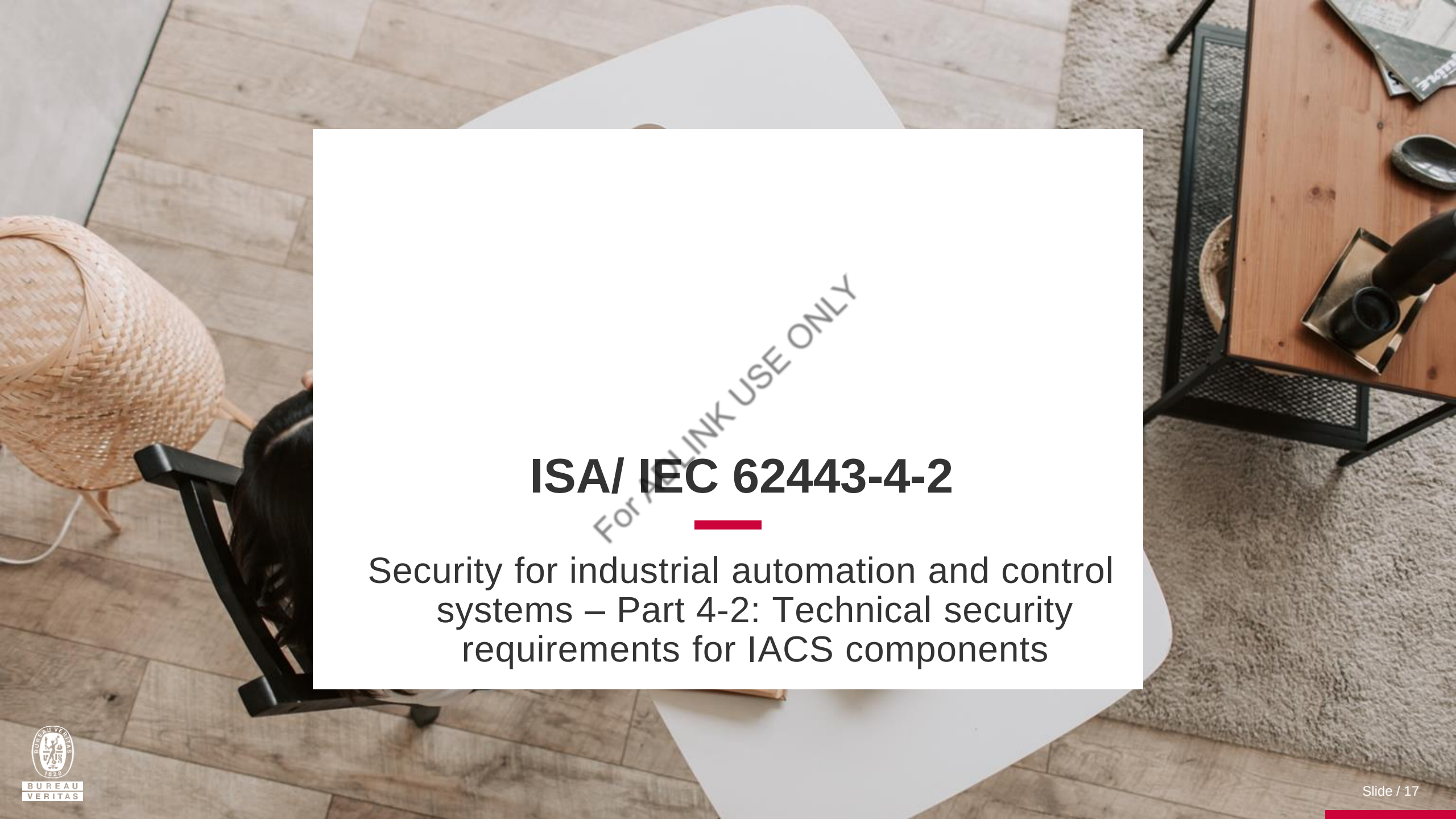
- **IEC 62443-2-4:2015/AMD1:2017**
- **IEC 62443-3-3:2013**
- **IEC 62443-4-1:2018**
- **IEC 62443-4-2:2019**

BUREAU VERITAS

ISASECURE STRATEGIC MEMBERS

For ADLINK USE ONLY

img src: https://isasecure.org/membership/current-members



For BV LINK USE ONLY

ISA/ IEC 62443-4-2

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

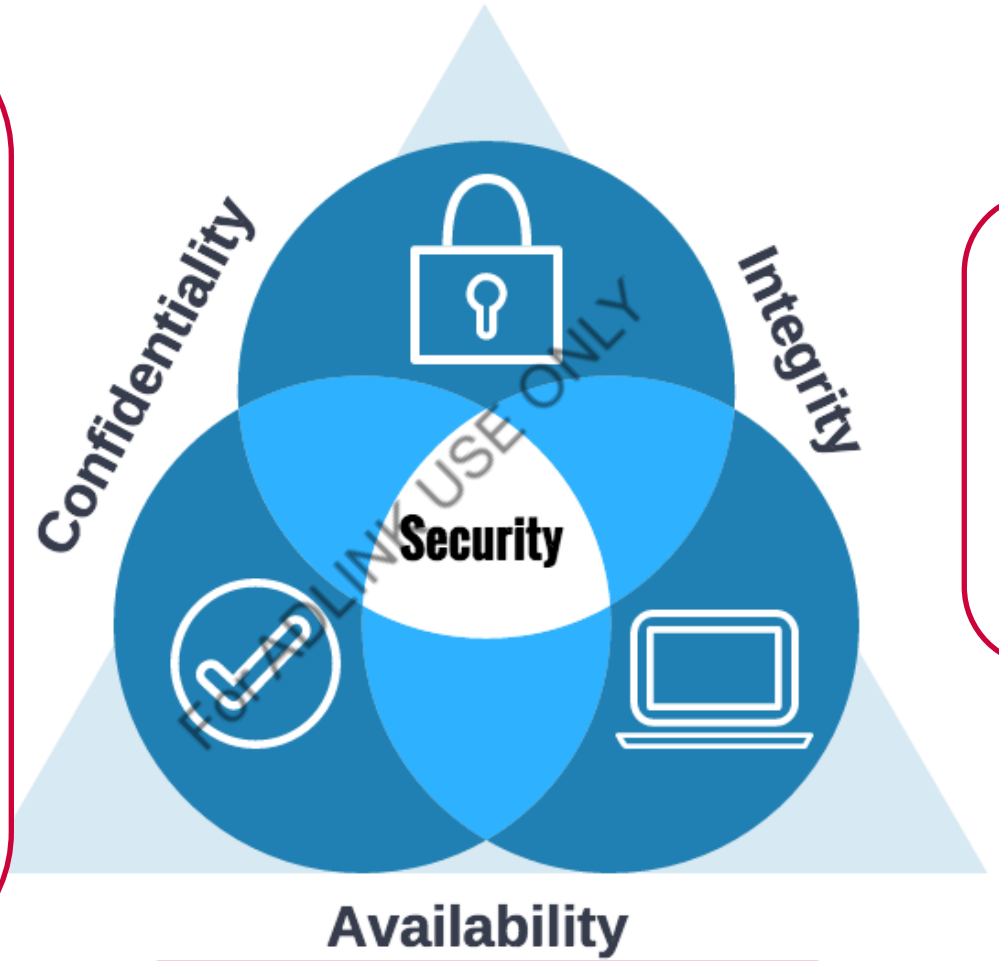
Timely response to evens
- Audit log accessibility
- Continuous monitoring

Identification and authentication control
- Human user/ software process identification and authentication
- Account management
- Strength of password-based authentication
- Unsuccessful login attempts
- Strength of public key-based authentication

Restricted Data Flow
- Network segmentation

Use Control
- Authorization enforcement
- Mobile code management
- Auditable events

Data Confidentiality
- Information confidentiality
- Information persistence
- Use of cryptography



FOR LINK USE ONLY

System Integrity
- Communication integrity
- Session integrity
- Update integrity
- Software and information integrity
- Support for update
- Physical tamper resistance and detection
- Integrity of the boot process

Resource Availability
- DoS protection
- Resource management
- Control system backup
- Control system component inventory

IEC62443-4-2 TECHNICAL SECURITY REQUIREMENTS FOR IACS COMPONENTS

Foundational Requirement

Identification and authentication control
Use control
System integrity
Data confidentiality
Restricted data flow
Timely response to evens
Resource availability

Component Requirement (CR)

Software Application Requirement (SAR)

Embedded Device Requirement (EDR)

Host Device Requirement (HDR)

Network Device Requirement (NDR)

For ADLINK USE ONLY

Device Type

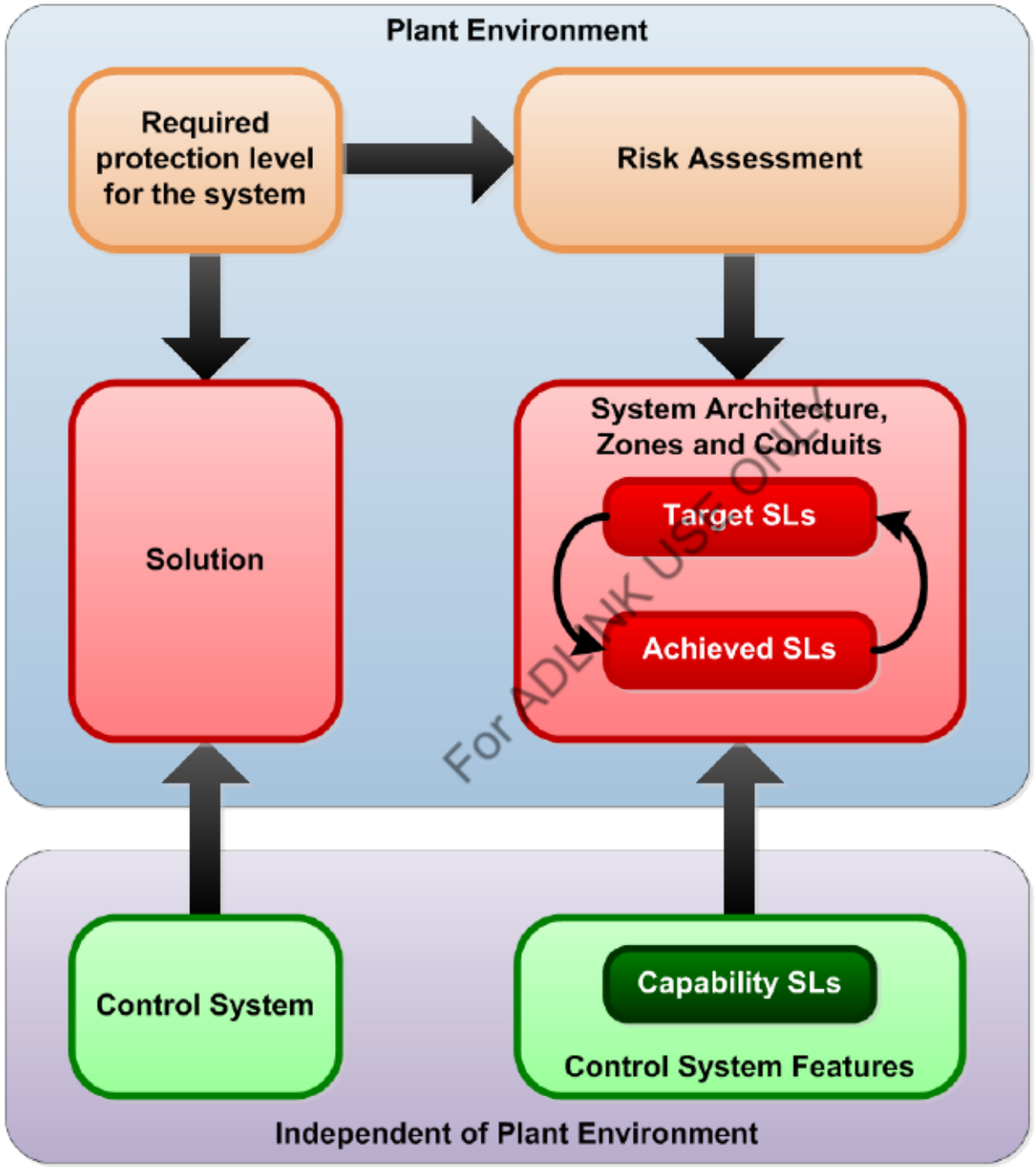
Host device	Embedded device	Network device	Software application
● general purpose device running an operating system (for example Microsoft Windows OS or Linux) capable of hosting one or more software applications, data stores or functions from one or more suppliers ● Note 1 to entry: Typical attributes include filesystem(s), programmable services, no real time scheduler and full HMI (keyboard, mouse, etc.).	● 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. ● Note 1 to entry: Typical attributes limited storage, limited number of exposed services, programmed through an external interface, embedded operating systems (OSs) or firmware equivalent, real-time scheduler, may have an attached control panel, and may have a communications interface.	● device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process ● Note 1 to entry: Typical attributes include embedded OS or firmware, no HMI, no real-time scheduler and configured through an external interface.	● 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) ● Note 1 to entry: Software applications typically execute on host devices or embedded devices. ● Note 2 to entry: Dependencies are any software programs that are necessary for the software application to function such as database packages, reporting tools, or any third party or open source software.

For ADLINK USE ONLY

Security Level	Description	Threat Actor	Examples of Actors
SL 1	Protection against casual or coincidental violation	Insider and/or External	• 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"	• 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		

For ADLINK USE ONLY

img src: https://orignix.com/wp-content/uploads/2020/09/blog3table-1.png



For ADLINK USE ONLY

Part 2-1
IACS security management System

and

Part 3-2
Zones and conduits

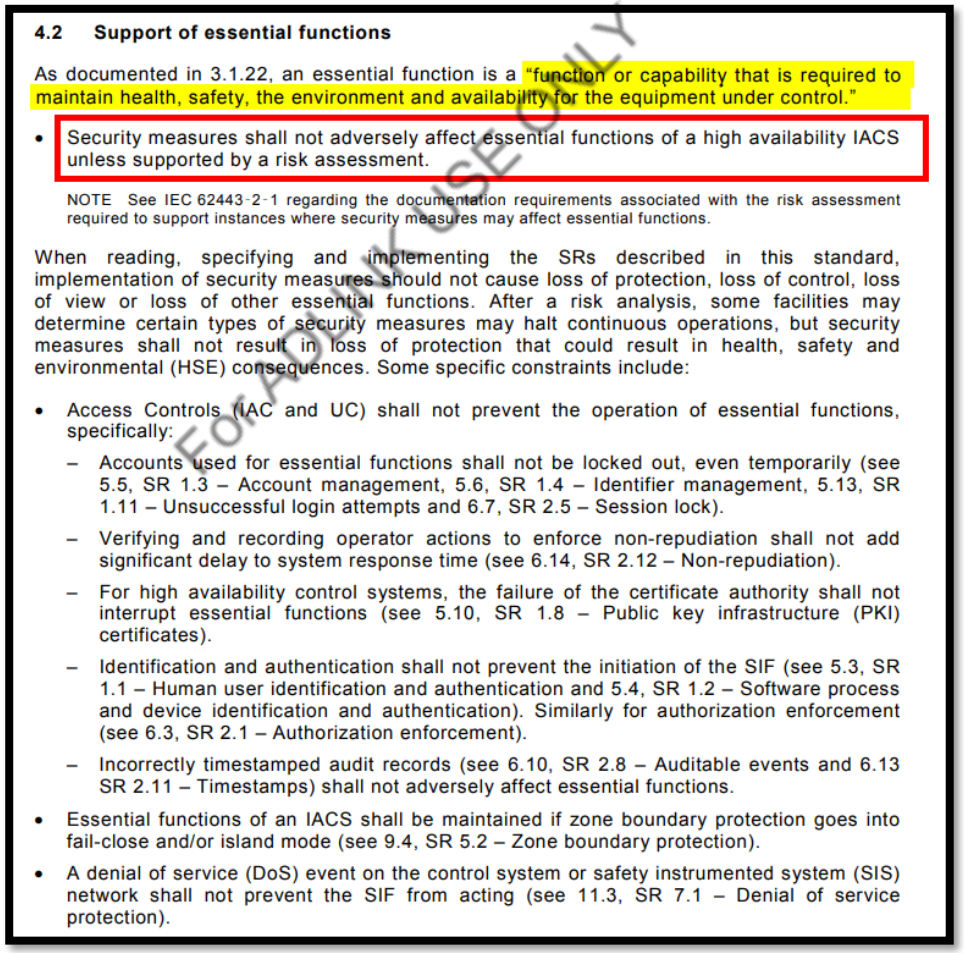
Part 3-3
System security requirements

Common component security constraints

For ADLINK USE ONLY

Common component security constraints

Requirement	Description
CCSC 1: Support of essential functions	系統的組件應遵循在 IEC 62443-3-3:2013 第 4 條中所描述的特定限制。



4.2 Support of essential functions

As documented in 3.1.22, an essential function is a "function or capability that is required to maintain health, safety, the environment and availability for the equipment under control."

- Security measures shall not adversely affect essential functions of a high availability IACS unless supported by a risk assessment.

NOTE See IEC 62443-2-1 regarding the documentation requirements associated with the risk assessment required to support instances where security measures may affect essential functions.

When reading, specifying and implementing the SRs described in this standard, implementation of security measures should not cause loss of protection, loss of control, loss of view or loss of other essential functions. After a risk analysis, some facilities may determine certain types of security measures may halt continuous operations, but security measures shall not result in loss of protection that could result in health, safety and environmental (HSE) consequences. Some specific constraints include:

- Access Controls (IAC and UC) shall not prevent the operation of essential functions, specifically:
  - Accounts used for essential functions shall not be locked out, even temporarily (see 5.5, SR 1.3 – Account management, 5.6, SR 1.4 – Identifier management, 5.13, SR 1.11 – Unsuccessful login attempts and 6.7, SR 2.5 – Session lock).
  - Verifying and recording operator actions to enforce non-repudiation shall not add significant delay to system response time (see 6.14, SR 2.12 – Non-repudiation).
  - For high availability control systems, the failure of the certificate authority shall not interrupt essential functions (see 5.10, SR 1.8 – Public key infrastructure (PKI) certificates).
  - Identification and authentication shall not prevent the initiation of the SIF (see 5.3, SR 1.1 – Human user identification and authentication and 5.4, SR 1.2 – Software process and device identification and authentication). Similarly for authorization enforcement (see 6.3, SR 2.1 – Authorization enforcement).
  - Incorrectly timestamped audit records (see 6.10, SR 2.8 – Auditable events and 6.13 SR 2.11 – Timestamps) shall not adversely affect essential functions.
- Essential functions of an IACS shall be maintained if zone boundary protection goes into fail-close and/or island mode (see 9.4, SR 5.2 – Zone boundary protection).
- A denial of service (DoS) event on the control system or safety instrumented system (SIS) network shall not prevent the SIF from acting (see 11.3, SR 7.1 – Denial of service protection).

For ANL IK USE ONLY

img src: ISA/ IEC 62443-3-3

Common component security constraints

Requirement	Description
CCSC 2: Compensating countermeasures	在某些情況下，若無外部補償性控制措施的幫助，可能無法滿足本文件中指定的一項或多項要求。當發生這樣的情況時，該組件的文件應該說明系統應用的適當補償性控制措施，以便在將該組件整合進系統時，能夠符合這些要求。

For ADLINK USE ONLY

Common component security constraints

Requirement	Description
CCSC 3: Least privilege	當需要且適宜時，一個或多個系統組件（包括軟體應用程式、嵌入式裝置、主機裝置和網路裝置）應該具備能力，讓系統執行最小權限原則。各別系統組件應提供足夠的權限細分和靈活性，將這些權限映射到角色上以支持該原則。當需要時，應可提供個人責任追究。權限的細分和分配取決於裝置類型，產品文件應在產品說明書中定義這一點。

For ADLINK USE ONLY

Common component security constraints

Requirement	Description
CCSC 4: Software development process	本文件中定義的所有組件應依照IEC 62443-4-1中描述的安全產品開發流程進行開發和支援。

For ADLINK USE ONLY

FR 1: Identification and authentication control (IAC)

For ADLINK USE ONLY

CR 1.1 – Human user identification and authentication

Requirement	Description	Security Level	Remarks
CR 1.1 Human user identification and authentication	組件應具備根據 IEC 62443-3-3 SR 1.1 標準，對所有能夠進行人員存取的介面進行用戶身份識別和鑑別的能力。該能力應在所有提供人員存取組件的介面上強制執行此類身份識別和鑑別，以支持職責分離和最小權限原則，符合相關的安全政策和流程。這項能力可以由組件本身提供，或通過整合到系統級別的身份識別和鑑別系統中來實現。	1,2,3,4	
CR 1.1 RE 1 – Unique identification and authentication	組件應具備能力以唯一地識別和鑑別所有人類使用者。	2,3,4	
CR 1.1 RE 2 – Multifactor authentication for all networks	組件應具備能力在通過所有網路存取控制系統時，為人類使用者採用多因子認證。	3,4	

For ADLINK USE ONLY

CR 1.2 – Software process and device identification and authentication

Requirement	Description	Security Level	Remarks
CR 1.2 – Software process and device identification and authentication	組件應具備能力自我識別並向其他組件（包括軟體應用、嵌入式裝置、主機裝置及網路裝置）進行鑑別，依據IEC 62443-3-3 SR1.2標準。若該組件，例如一個應用程式，在人類用戶的背景下運行，此外，根據IEC 62443-3-3 SR1.1標準的人類用戶識別與鑑別可能是組件對其他組件識別與鑑別過程的一部分。	2,3,4	
CR 1.2 RE 1 – Unique identification and authentication	組件應提供向任何其他組件唯一識別和鑑別自身的能力。	3,4	

For ADLINK use only

CR 1.3 – Account management

Requirement	Description	Security Level	Remarks
CR 1.3 – Account management	組件應具備能力，直接或透過整合至系統中來管理所有帳戶，符合 IEC 62443-3-3 SR 1.3 標準。	1,2,3,4	

For ADLINK USE ONLY

5.5 SR 1.3 – Account management

5.5.1 Requirement

The control system shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing accounts.

img src: ISA/ IEC 62443-3-3

CR 1.4 – Identifier management

Requirement	Description	Security Level	Remarks
CR 1.4 – Identifier management	組件應具備能力，直接或透過整合至系統中，來支援管理識別碼，符合 IEC 62443-3-3 SR 1.4 標準。	1,2,3,4	

FOR ADLINK USE ONLY

5.6 SR 1.4 – Identifier management

5.6.1 Requirement

The control system shall provide the capability to support the management of identifiers by user, group, role or control system interface.

img src: ISA/ IEC 62443-3-3

CR 1.5 – Authenticator management

Requirement	Description	Security Level	Remarks
CR 1.5 – Authenticator management	組件應具備以下能力： a) 支援使用初始鑑別因子內容； b) 支援在安裝時識別對預設鑑別因子所做的更改; c) 能夠在定期更改/更新鑑別因子時正常運作； d) 在儲存、使用和傳輸時，保護鑑別因子不受未授權的揭露和修改。	1,2,3,4	
CR 1.5 RE 1 – Hardware security for authenticators	組件所依賴的鑑別因子應通過硬體機制進行保護。 例如：密碼保護記憶體、一次性密碼（OTP）記憶體、硬體資料完整性檢查，以及裝置安全啟動機制。	3,4	

For ADLINK USE ONLY

CR 1.7 – Strength of password-based authentication

Requirement	Description	Security Level	Remarks
CR 1.7 – Strength of password-based authentication	對於使用密碼鑑別的組件，這些組件應提供或整合到一個系統中，該系統具備根據國際公認且經過認可的密碼指引強制執行可配置密碼強度的能力。	1,2,3,4	
CR 1.7 RE 1 – Password generation and lifetime restrictions for human users	組件應提供或整合到一個系統中，該系統能夠防止任何特定人類用戶帳戶在可設定的幾代之內重複使用密碼。此外，組件應提供強制執行人類用戶密碼最短和最長使用期限限制的能力。這些功能應符合普遍接受的安全行業慣例。組件應提供在密碼過期前一個可設定的時間內提示用戶更改密碼的能力。	3	
CR 1.7 RE 2 – Password lifetime restrictions for all users (human, software process, or device)	組件應提供或整合到一個系統中，該系統能夠強制執行所有用戶的密碼最短和最長使用期限限制。	4	

FOR ADVANCE USE ONLY

CR 1.8 – Public key infrastructure certificates

Requirement	Description	Security Level	Remarks
CR 1.8 – Public key infrastructure certificates	當使用公開金鑰基礎設施（PKI）時，組件應提供或整合到一個系統中，該系統能夠與IEC 62443-3-3 SR1.8相互作用並按其規定運行。	2,3,4	

For ADLINK USE ONLY

5.10 SR 1.8 – Public key infrastructure (PKI) certificates

5.10.1 Requirement

Where PKI is utilized, the control system shall provide the capability to operate a PKI according to commonly accepted best practices or obtain public key certificates from an existing PKI.

img src: ISA/ IEC 62443-3-3

CR 1.9 – Strength of public key authentication

Requirement	Description	Security Level	Remarks
CR 1.9 – Strength of public key authentication	針對使用公開金鑰鑑別的組件，這些組件應直接提供或整合到一個系統中，該系統在相同的IACS環境中具有以下能力： a) 通過檢查給定證書的簽名有效性來驗證證書； b) 驗證證書鏈，或在自簽名證書的情況下，通過向所有與證書主體進行通訊的主機部署葉證書； c) 通過檢查給定證書的吊銷狀態來驗證證書； d) 建立用戶（人類、軟體程式或設備）對相應私鑰的控制； e) 將驗證後的身份映射到用戶（人類、軟體程式或設備）； f) 確保用於公開金鑰驗證的算法和密鑰符合8.5條款的要求。	2,3,4	
CR 1.9 RE 1 – Hardware security for public key-based authentication	組件應提供通過硬體機制保護關鍵、長期有效私鑰的能力。	3,4	

FOR DLNK USE ONLY

CR 1.10 – Authenticator feedback

Requirement	Description	Security Level	Remarks
CR 1.10 – Authenticator feedback	當組件提供鑑別功能時，該組件應提供在鑑別過程中隱藏鑑別資訊回饋的能力。	1,2,3,4	

For ADLINK USE ONLY

CR 1.11 – Unsuccessful login attempts

Requirement	Description	Security Level	Remarks
CR 1.11 – Unsuccessful login attempts	當組件提供鑑別功能時，該組件應提供以下能力： a) 在可設定的時間段內，對任何用戶（人員、軟體程式或設備）實行連續無效存取嘗試的次數上限； b) 當達到此次數上限時，拒絕存取一段指定時間，或直到由管理員解鎖。在期限到期之前，管理員可以提前解鎖帳號。	1,2,3,4	

For ADL Use Only

CR 1.12 – System use notification

Requirement	Description	Security Level	Remarks
CR 1.12 – System use notification	當組件提供本地人類用戶存取 HMI 時，應具備在進行鑑別前顯示系統使用通知訊息的能力。該系統使用通知訊息應可由授權人員設定。	1,2,3,4	

For ADLINK USE ONLY

CR 1.14 – Strength of symmetric key-based authentication

Requirement	Description	Security Level	Remarks
CR 1.14 – Strength of symmetric key-based authentication	對於使用對稱金鑰的組件，該組件應具備以下能力： a) 使用對稱金鑰建立相互信任； b) 安全地儲存共享的秘密（只要共享的秘密保持機密，鑑別即有效） c) 限制對共享秘密的存取；以及 d) 確保用於對稱金鑰鑑別的算法和鑰匙符合8.5條款要求。	2,3,4	
CR 1.14 RE 1 – Hardware security for symmetric key-based authentication	組件應具備透過硬體機制保護關鍵、長期使用對稱金鑰的能力。	3,4	

For ADLINK USE ONLY

FR 2: Use Control

For ADLINK IN-HOUSE ONLY

CR 2.1 – Authorization enforcement

Requirement	Description	Security Level	Remarks
CR 2.1 – Authorization enforcement	組件應提供一種授權執行機制，用於根據已確認和經鑑別的使用者之指派職責進行控制。	1,2,3,4	
CR 2.1 RE 1 – Authorization enforcement for all users	組件應提供一種授權執行機制，用於基於所有使用者（包括人類、軟體程式和裝置）的指派職責和最小特權原則。	2,3,4	
CR 2.1 RE 2 – Permission mapping to roles	組件應直接或透過補償安全機制，允許授權角色定義和修改所有人類使用者的權限至角色的映射。角色不應僅限於固定的階層級結構。	2,3,4	
CR 2.1 RE 3 – Supervisor override	組件應支援監督者的手動覆寫功能，可設定時間或事件序列。	3,4	
CR 2.1 RE 4 – Dual approval	當行為可能對工控流程造成嚴重影響時，組件應支援雙重批准。雙重批准應限於需要極高信心水平來可靠、正確執行的行為。	4	

BV-PLINK USE ONLY

CR 2.2 – Wireless use control

Requirement	Description	Security Level	Remarks
CR 2.2 – Wireless use control	如果組件支援透過無線介面的使用，則應提供整合到系統的能力，以支援使用授權、監控和限制，並符合公認的業界實例。	1,2,3,4	

For ADLINK USE ONLY

HDR 2.4 – Mobile code

Requirement	Description	Security Level	Remarks
HDR 2.4 – Mobile code	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： 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	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。	2,3,4	

PANDLINK USE ONLY

CR 2.5 – Session lock

Requirement	Description	Security Level	Remarks
CR 2.5 – Session lock	若組件提供人類用戶介面，無論是本地存取還是通過網路存取，該組件應提供以下能力： a) 在無活動的可設定時間段後或通過用戶（人類、軟體程式或裝置）手動啟動後，透過啟動會話鎖定來防止進一步存取；以及 b) 會話鎖定應保持有效，直到擁有會話的人類用戶或另一位授權的人類用戶，使用適當的身份識別和鑑別程序重新建立存取。	1,2,3,4	

BU ADLINK USE ONLY

CR 2.6 – Remote session termination

Requirement	Description	Security Level	Remarks
CR 2.6 – Remote session termination	若組件支持遠端會話，該組件應提供能力，以在無活動的可設定時間段後自動終止遠端會話，或由本地授權人員手動終止，或由啟動該會話的用戶（人類、軟體程序或裝置）手動終止。	2,3,4	

For ADLINK USE ONLY

CR 2.7 – Concurrent session control

Requirement	Description	Security Level	Remarks
CR 2.7 – Concurrent session control	組件應提供限制任何特定用戶（人類、軟體程序或裝置）在每個介面上的並行會話數量的能力。	3,4	

For ADLINK USE ONLY

CR 2.8 – Auditable events

Requirement	Description	Security Level	Remarks
CR 2.8 – Auditable events	組件應提供生成與安全相關的審計記錄的能力，涵蓋以下類別： a) 存取控制； b) 請求錯誤； c) 控制系統事件； d) 備份與恢復事件； e) 設定更改；以及 f) 審計日誌事件。 單獨的審計記錄應包括： a) 時間戳記； b) 來源（起始裝置、軟體程式或人類帳戶）； c) 類別； d) 類型； e) 事件 ID；以及 f) 事件結果。	1,2,3,4	

For DLINK USE ONLY

CR 2.9 – Audit storage capacity

Requirement	Description	Security Level	Remarks
CR 2.9 – Audit storage capacity	組件應： a) 提供根據常見的日誌管理建議分配審計記錄存儲容量的能力；以及 b) 提供機制來防止組件在達到或超過審計存儲容量時失敗。	1,2,3,4	
CR 2.9 RE 1 – Warn when audit record storage capacity threshold reached	組件應提供當分配的記錄存儲容量達到可調整之最大記錄存儲容量時發出警告的能力。	3,4	

For ADLINK USE ONLY

CR 2.10 – Response to audit processing failures

Requirement	Description	Security Level	Remarks
CR 2.10 – Response to audit processing failures	組件應： a) 提供在審計處理失敗時防止失去關鍵服務和功能的能力；以及 b) 根據普遍接受的行業實踐和建議，提供支持對審計處理失敗做出適當反應的能力。	1,2,3,4	

For ADLINK USE ONLY

CR 2.11 – Timestamps

Requirement	Description	Security Level	Remarks
CR 2.11 – Timestamps	組件應提供建立時間戳記（包括日期和時間）的能力，用於審計記錄。	1,2,3,4	
CR 2.11 RE 1 – Time synchronization	組件應提供與系統時間源同步的時間戳記建立能力。	2,3,4	
CR 2.11 RE 2 – Protection of time source integrity	時間同步機制應提供檢測未經授權修改的能力，並在修改時引發審計事件。	4	

For ADLINK USE ONLY

CR 2.12 – Non-repudiation

Requirement	Description	Security Level	Remarks
CR 2.12 – Non-repudiation	若組件提供人類使用者介面，則該組件應具備確定特定人類使用者是否執行特定操作的能力。無法支援此能力的控制元素應列於組件文件中。	1,2,3,4	
CR 2.12 RE 1 – Non-repudiation for all users	組件應具備能力以判斷指定的使用者（人類、軟體程式或設備）是否執行了特定操作。	4	

For ADLINK USE ONLY

HDR 2.13 – Use of physical diagnostic and test interfaces

Requirement	Description	Security Level	Remarks
HDR 2.13 – Use of physical diagnostic and test interfaces	主機設備應防止未經授權使用實體工廠診斷和測試介面（例如 JTAG 除錯介面）。	2,3,4	
HDR 2.13 RE 1 – Active monitoring	主機設備應提供診斷和測試介面的主動監控，並在檢測到嘗試存取這些介面時生成審計日誌條目。	3,4	

For ADLINK USE ONLY

FR 3 – System integrity

For ADLINK USE ONLY

CR 3.1 – Communication integrity

Requirement	Description	Security Level	Remarks
CR 3.1 – Communication integrity	組件應提供保護傳輸資訊完整性的能力。	1,2,3,4	
CR 3.1 RE 1 – Communication authentication	組件應提供在通訊過程中驗證接收資訊真實性的能力。 注意：無需提供保密性保護即可達成資訊完整性保護和來源鑑別。	2,3,4	

For ADLINK USE ONLY

HDR 3.2 – Protection from malicious code

Requirement	Description	Security Level	Remarks
HDR 3.2 – Malicious code protection	主機裝置上應有由 IACS 產品供應商認證的機制，用於防範惡意程式碼。IACS 產品供應商應記錄與防範惡意程式碼相關的任何特殊配置要求。	1,2,3,4	
HDR 3.2 RE 1 – Report version of code protection	主機裝置應自動報告正在使用的防範惡意程式碼的軟體和文件版本（作為整體記錄功能的一部分）。	2,3,4	

For ADLINK USE ONLY

CR 3.3 – Security functionality verification

Requirement	Description	Security Level	Remarks
CR 3.3 – Security functionality verification	組件應提供支援根據 IEC 62443-3-3 SR3.3 驗證安全功能預期操作的能力。	1,2,3,4	
CR 3.3 RE 1 – Security functionality verification during normal operation	組件應提供在正常運作期間支援驗證安全功能預期操作的能力。這項要求需要謹慎實施，以避免產生不良影響。對於安全系統而言，這可能不適用。	4	

For ADLINK USE ONLY

7.5 SR 3.3 – Security functionality verification

7.5.1 Requirement

The control system shall provide the capability to support verification of the intended operation of security functions and report when anomalies are discovered during FAT, SAT and scheduled maintenance. These security functions shall include all those necessary to support the security requirements specified in this standard.

img src: ISA/ IEC 62443-3-3

CR 3.4 – Software and information integrity

Requirement	Description	Security Level	Remarks
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	

For ADLINK USE ONLY

CR 3.5 – Input validation

Requirement	Description	Security Level	Remarks
CR 3.5 – Input validation	組件應驗證用作工業過程控制輸入或通過外部介面直接影響組件行為的任何輸入資料的語法、長度和內容。	1,2,3,4	

For ADLINK USE ONLY

CR 3.6 – Deterministic output

Requirement	Description	Security Level	Remarks
CR 3.6 – Deterministic output	連接到自動化過程的組件應具備能力，在無法維持由組件供應商定義的正常運作時，將輸出設置為預定義狀態。	1,2,3,4	

For ADLINK USE ONLY

CR 3.7 – Error handling

Requirement	Description	Security Level	Remarks
CR 3.7 – Error handling	控制系統應以有效的方式辨別和處理錯誤狀況，以便進行有效的修復。除非為了及時解決問題而需要揭示這些資訊，否則不應提供攻擊者可以利用來攻擊 IACS 的資訊。	1,2,3,4	

For ADLINK USE ONLY

CR 3.8 – Session integrity

Requirement	Description	Security Level	Remarks
CR 3.8 – Session integrity	組件應提供機制來保護通訊會話的完整性，包括： a) 在用戶登出或其他會話終止時（包括瀏覽器會話）使會話識別碼失效的能力； b) 為每個會話生成唯一會話識別碼，並僅識別系統生成的會話識別碼的能力；以及 c) 使用公認的隨機源生成唯一會話識別碼的能力。	2,3,4	

For ADLINK USE ONLY

CR 3.9 – Protection of audit information

Requirement	Description	Security Level	Remarks
CR 3.9 – Protection of audit information	組件應保護審計資訊、審計日誌和審計工具（如果存在）免受未經授權的存取、修改和刪除。	2,3,4	
CR 3.9 RE 1 – Audit records on write-once media	組件應提供能力，在硬體強制的一次性寫入媒體上儲存審計記錄。	4	

For ADLINK USE ONLY

HDR 3.10 – Support for updates

Requirement	Description	Security Level	Remarks
HDR 3.10 – Support for updates	主機裝置應支援更新和升級的能力。	1,2,3,4	
HDR 3.10 RE 1 – Update authenticity and integrity	主機裝置在安裝任何軟體更新或升級之前，應驗證其真實性和完整性。	2,3,4	

For ADLINK USE ONLY

HDR 3.11 – Physical tamper resistance and detection

Requirement	Description	Security Level	Remarks
HDR 3.11 – Physical tamper resistance and detection	主機裝置應提供支援抗篡改和檢測機制的能力，以防止未經授權的物理存取該裝置。	2,3,4	
HDR 3.11 RE 1 – Notification of a tampering attempt	主機裝置應能在發現未經授權的實體存取嘗試時，自動向可設定的接收者群發出通知。所有篡改通知應作為整體審計日誌功能的一部分記錄下來。	3,4	

For ADLINK USE ONLY

HDR 3.12 – Provisioning product supplier roots of trust

Requirement	Description	Security Level	Remarks
HDR 3.12 – Provisioning product supplier roots of trust	主機裝置應提供在製造時配置和保護產品供應商密鑰和資料的能力，以確保其保密性、完整性和真實性，並將其作為一個或多個“信任根”。	2,3,4	

For ADLINK USE ONLY

HDR 3.13 – Provisioning asset owner roots of trust

Requirement	Description	Security Level	Remarks
HDR 3.13 – Provisioning asset owner roots of trust	主機裝置應： a) 提供設定和保護資產擁有者密鑰和資料的保密性、完整性和真實性的能力，這些資料用作“信任根源”；以及 b) 支援在不依賴設備安全區域以外的組件情況下進行設定的能力。。	2,3,4	

For ADLINK USE ONLY

HDR 3.14 – Integrity of the boot process

Requirement	Description	Security Level	Remarks
HDR 3.14 – Integrity of the boot process	主機裝置應在啟動過程中使用之前，驗證韌體、軟體和設定檔的完整性，以確保其在啟動過程中的可靠性。	1,2,3,4	
HDR 3.14 RE 1 – Authenticity of the boot process	主機裝置應在啟動過程中使用之前，驗證韌體、軟體和設定檔的完整性，以確保其在啟動過程中的可靠性。	2,3,4	

For ADLINK USE ONLY

FR 4 – Data confidentiality

For ADLINK USE ONLY

CR 4.1 – Information confidentiality

Requirement	Description	Security Level	Remarks
CR 4.1 – Information confidentiality	組件應提供以下功能： a) 保護支援明確的讀取授權的資訊在儲存狀態下的機密性。 b) 支援資訊在傳輸過程中的機密性保護，符合IEC 62443-3-3 SR 4.1的定義。	1,2,3,4	

FOR ADLINK USE ONLY

8.3 SR 4.1 – Information confidentiality

8.3.1 Requirement

The control system shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit.

img src: ISA/ IEC 62443-3-3

CR 4.2 – Information persistence

Requirement	Description	Security Level	Remarks
CR 4.2 – Information persistence	組件將要被停用和/或退役時，組件應提供刪除所有資訊的能力，對於這些資訊有明確的讀取授權。	2,3,4	
CR 4.2 RE 1 – Erase of shared memory resources	組件應提供保護措施，以防止通過揮發性共享記憶資源進行未經授權和意外的資訊傳輸。 揮發性記憶資源通常在釋放給記憶管理後不會保留資訊。然而，存在針對隨機訪問記憶體（RAM）的攻擊，可能在實際覆寫之前提取密鑰材料或其他機密資料。因此，當揮發性共享記憶資源被釋放供不同使用者使用時，需要從資源中清除所有獨特的資料和與獨特資料的連接，讓新使用者不可讀取或存取。	3,4	
CR 4.2 RE 2 – Erase verification	組件應提供驗證資訊刪除的能力。	3,4	

For ADLINK use only

CR 4.3 – Use of cryptography

Requirement	Description	Security Level	Remarks
CR 4.3 – Use of cryptography	如果需要加密，組件應使用根據國際公認和經過驗證的安全實踐和建議的加密安全機制 。	1,2,3,4	

For ADLINK USE ONLY

FR 5 – Restricted data flow

For ADLINK USE ONLY

CR 5.1 – Network segmentation

Requirement	Description	Security Level	Remarks
CR 5.1 – Network segmentation	組件應支援分段網路，根據邏輯分段和重要性的需要，以滿足更廣泛的網路架構。 這包括支援不同區域和通道的設置，以確保網路的安全性和可靠性。	1,2,3,4	

For ADLINK USE ONLY

FR 6 – Timely response to events

For ADLINK USE ONLY

CR 6.1 – Audit log accessibility

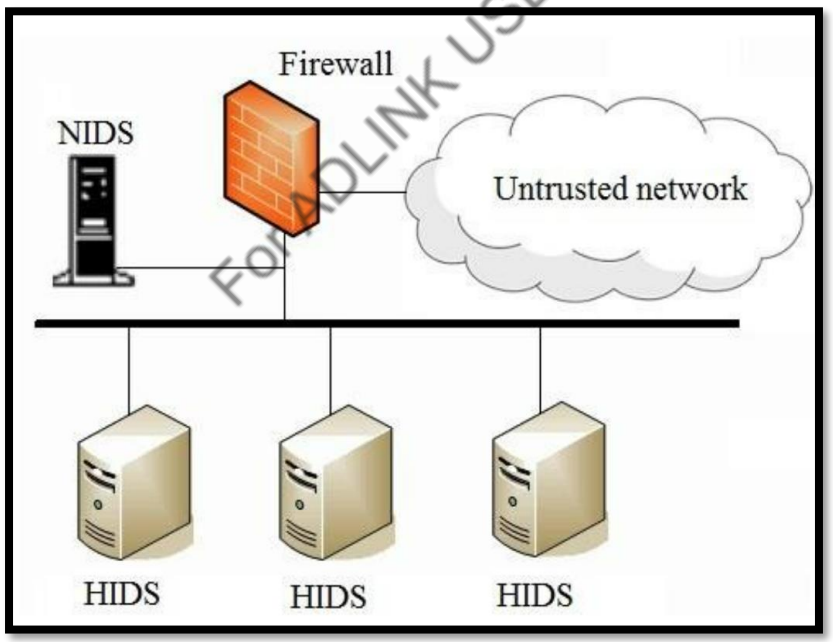
Requirement	Description	Security Level	Remarks
CR 6.1 – Audit log accessibility	組件應提供授權的人員和/或工具以唯讀方式存取稽核日誌的能力。	1,2,3,4	
CR 6.1 RE 1 – Programmatic access to audit logs	組件應透過使用應用程式介面（API）或將審計記錄傳送到集中系統來提供對審計記錄的程式存取。這樣可以方便地進行稽核和監視，以確保系統的安全性和合規性。	3,4	

For ADLINK USE ONLY

CR 6.2 – Continuous monitoring

Requirement	Description	Security Level	Remarks
CR 6.2 – Continuous monitoring	組件應提供連續監控的能力，採用廣泛接受的安全行業實踐和建議，以及及時檢測、描述和報告安全漏洞。這意味著組件應該能夠不斷地被監視，以迅速識別和回報任何安全違規行為，並採取相應的措施。	2,3,4	

For ADLINK USE ONLY



img src: https://www.researchgate.net/figure/Illustrates-the-implementation-of-both-NIDS-and-HIDS-to-protect-the-network_fig1_332524050

FR 7 – Resource availability

For ADLINK USE ONLY

CR 7.1 – Denial of service protection

Requirement	Description	Security Level	Remarks
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	

For ADLINK USE ONLY

CR 7.2 – Resource management

Requirement	Description	Security Level	Remarks
CR 7.2 – Resource management	組件應提供限制安全功能使用資源的能力，以防止資源耗盡。	1,2,3,4	

For ADLINK USE ONLY

CR 7.3 – Control system backup

Requirement	Description	Security Level	Remarks
CR 7.3 – Control system backup	組件應提供參與系統級備份操作的能力，以保護組件狀態 (user- and system-level information)。備份過程不應影響正常的組件運作。	1,2,3,4	
CR 7.3 RE 1 – Backup integrity verification	組件應提供驗證備份資訊完整性的能力，在恢復資訊之前對其進行驗證。	2,3,4	

For ADLINK USE ONLY

CR 7.4 – Control system recovery and reconstitution

Requirement	Description	Security Level	Remarks
CR 7.4 – Control system recovery and reconstitution	組件應提供在中斷或故障後恢復並重組至已知安全狀態的能力。	1,2,3,4	

For ADLINK USE ONLY

CR 7.6 – Network and security configuration settings

Requirement	Description	Security Level	Remarks
CR 7.6 – Network and security configuration settings	組件應提供根據控制系統供應商提供的指引所描述的推薦網路和安全配置進行配置的能力。該組件應提供一個介面，用於當前部署的網路和安全設定。	1,2,3,4	
CR 7.6 RE 1 – Machine-readable reporting of current security settings	組件應提供能力，生成一份報告，列出當前部署的安全設定，並以機器可讀的格式呈現。	3,4	

For ADLINK USE ONLY

CR 7.7 – Least functionality

Requirement	Description	Security Level	Remarks
CR 7.7 – Least functionality	組件應提供專門限制不必要的功能、連接埠、協定和/或服務的使用的能力。	1,2,3,4	

For ADLINK USE ONLY

CR 7.8 – Control system component inventory

Requirement	Description	Security Level	Remarks
CR 7.8 – Control system component inventory	組件應提供支援符合 IEC 62443-3-3 SR 7.8 的控制系統組件盤點的能力。	2,3,4	

For ADLINK USE ONLY

11.10 SR 7.8 – Control system component inventory

11.10.1 Requirement

The control system shall provide the capability to report the current list of installed components and their associated properties.

img src: ISA/ IEC 62443-3-3

Any Questions?

For ADLINK USE ONLY

THANK YOU

For ADLINK USE ONLY