



# 為企業的網路和資訊安全保駕護航 Digital Enterprise. Protected.

您的資訊和網路安全全球合作夥伴




Your Global Partner for Information and Cybersecurity

[www.tuv.com](http://www.tuv.com)

 **TÜVRheinland®**  
Precisely Right.

# 網路安全服務解決方案：完善並通行全球

## Our complete, global cybersecurity portfolio

服務類別 PORTFOLIO CATEGORIES	服務內容 SERVICE LINES	服務類型 SERVICE TYPES
<b>掌控風險與合規管理</b> <b>MASTERING RISK &amp; COMPLIANCE</b>	管理與策略 Government & Strategy	業務持續性管理 Business Continuity Management
	風險與合規管理 Risk & Compliance Management	資料隱私保護 Data Privacy
	資訊安全管理系統 Information Security Management Systems	
<b>先進的網路防禦</b> <b>ADVANCED CYBER DEFENSES</b>	身份識別與准入管理 Identity & Access Management	物聯網安全 IoT Security
	網路安全 Network Security	工業安全 Industrial Security
	應用安全 Application Security	安全分析和風險識別 Security Analytics & Detection
	終端安全 Endpoint Security	突發事件回應 Incident Response
	資料保護 Data Protection	
<b>雲安全應用</b> <b>SECURE CLOUD ADOPTION</b>	雲安全 Cloud Security	
	企業私有雲 Enterprise Cloud Adoption	
	混合雲 Hybrid Infrastructure	
		<b>諮詢服務</b> <b>CONSULTING SERVICES</b> 
		<b>測試服務</b> <b>TESTING SERVICES</b> 
		<b>管理服務</b> <b>MANAGED SERVICES</b> 

- 全球一致的系列服務，助力您的企業獲得戰略指導、驗證流程和一流技術，以有效地管理風險，保護關鍵資產，這在數字化時代具有深遠的意義。

**A globally consistent portfolio**, that is far-reaching and equally deep, gives your organization access to the strategic guidance, proven processes and best-in-class technology necessary to effectively manage risk, protect critical assets and thrive in the digital era.

- 單一服務提供者，使公司組織內完整的端到端的網路安全告別複雜流程，最大限度地降低營運費用，加快數位化轉型。

**A single source** for your organization's complete, end-to-end cybersecurity needs simplified processes, minimizes operating expenses and helps accelerate your digital transformation.

- 以服務為導向，助您把握全域，做出明智、可行以及高性價比的決策。

**A service-orientated approach** helps you see the full picture and make informed, actionable and cost-efficient decisions.

- 全方位自上而下的系列服務，確保每個利益相關方（從公司的管理層到技術操作人員）都參與到該流程中，以確保各方長期齊心協力、持續協作。

**A comprehensive, top-down portfolio approach** ensures each stakeholder, from your organization's C-level leaders to its technical security practitioners, are involved and engaged in the process to ensure necessary buy-in, ongoing collaboration and long-term success.

- 我們的端對端諮詢、測試和管理服務是最先進的前瞻性解決方案，可幫助您始終保持領先和競爭力。

**Our end-to-end consulting, testing and managed services** are state-of-the-art, forward-looking solutions that help you always stay ahead and competitive.

- 我們所有服務可以在全球範圍內提供，從諮詢、解決方案的實施到管理服務等。

**All of our services can be provided worldwide**, from consulting, implementation of solutions to managed services.

# 協助您的智慧產品應對 GDPR 法規

## Expertise in solutions for GDPR-compliant smart products

歐盟《通用資料保護法案》(GDPR) 是迄今為止覆蓋面最廣的全球性資料隱私保護法規，該法案於 2018 年 5 月 25 日強制生效。任何在歐盟區域銷售產品或者提供服務的廠商以及組織，涉及處理歐洲公民個人資料的都必須遵守該條例。不合規的企業可能面臨高達 2000 萬歐元或 4% 年營業額的罰款，最終金額將選取兩者最高值。

德國萊因 TÜV 是智慧產品一站式解決方案專家，從產品研發到市售階段，提供詳盡的測試以及評估服務，明客戶應對全新 GDPR 法案。

The European Union's General Data Protection Regulation (GDPR) has been designed to safeguard data privacy, covering the widest scope of data protection in that regard. It comes into force on 25 May 2018. Any organisation that sells products or provides services in the EU and deals with EU citizens' personal data must abide by the GDPR. Violators may face fines of up to €20 million or up to 4% of their annual worldwide turnover, whichever is greater.

With expertise in one-stop solutions for smart products, TÜV Rheinland provides testing and consulting services from product design to marketing and can help clients comply with the GDPR.

### 我們的服務 OUR SERVICE

- IoT 產品與服務的隱私保護驗證  
Certification of Internet of Things products and services privacy protection
- IoT 產品與服務解決方案評估  
IoT products and service solutions assessment

### 品範 PRODUCT SCOPE

- IoT 智慧物聯網產品      IoT products
- 智慧穿戴設備              Smart wearable devices
- 智慧家居產品                Smart home
- 智慧車載產品                Smart vehicle systems
- 智慧攝像頭                  Smart cameras
- 智慧電視                      Smart TVs

### 服務流程 SERVICE PROCEDURES



# 工業自動化網路安全解決方案

## Cybersecurity in industrial automation

越來越多的生產和流程自動化工業控制系統正在接入企業內外部網路。跟隨不同的安全系統和網路間的資料傳輸而來的，是被攻擊和故障的易感性。因此，十分必要阻止內外部無授權的訪問，進而確保控制系統的可用性和完整性。

Industrial control systems for manufacturing and process automation are increasingly implemented within internal and external company networks. Thus data transfer between differently safe systems and networks arises, increasing susceptibility for attacks and failures. It is necessary to prevent internal and external unauthorized access in order to ensure the availability and integrity of control systems.

### 功能安全和網路資訊安全

#### FUNCTIONAL SAFETY AND CYBER SECURITY

- 網路資訊安全相關的自動化解決方案在功能必須上是安全的（功能安全）。  
Safety-related automation solutions must be functionally safe (Functional Safety).
- 資訊安全的目標是資料和功能的可用性、完整性和機密性。  
The objective of security is the availability, integrity and confidentiality of data and functions.
- 除了針對元件單元進行功能安全評估外，德國萊因 TÜV 還提供基於網路安全要求的綜合產品測試。  
In addition to qualifying components against Functional Safety, TÜV Rheinland offers combined product testing considering requirements regarding cybersecurity.
- 國際通用標準 IEC 62443 和 ISASecure™ 系列標準的要求皆根據安全生命週期以及功能要求制定。  
Requirements of the internationally accepted standard IEC 62443 and the series of standard ISASecure™ are considered in terms of a security life cycle as well as the functional requirements.



Functional  
Safety  
Cyber Security

www.tuv.com  
ID 0600000000



## 測試標誌：「功能安全 / 網路資訊安全」

### TEST MARK : "FUNCTIONAL SAFETY / CYBERSECURITY"

德國萊因 TÜV 的「功能安全與資訊安全」測試標誌適用於電子電氣可程式設計控制系統產品，這些產品將應用於安全相關領域。根據 IEC 62443 標準要求，特定產品的製造商需要採取相應措施。

The test mark "Functional Safety and Cybersecurity" of TÜV Rheinland is applied to electronic / programmable electronic products, which are applied in safety-related applications. Manufacturers of such products additionally need to apply measures according to the requirements of the standard IEC 62443.

除功能安全標準外，資訊安全相關標準還包括：

Apart from the Functional Safety standards the requirements of the following standards are relevant:

- IEC 62443-3-3：工業通信網路 – 網路與系統安全  
第 3-3 部分：系統安全要求和安全級別  
IEC 62443-3-3: Industrial communication networks  
Network and system security  
Part 3-3: System security requirements and security levels
- IEC 62443-4-1：工業通信網路 – 網路與系統安全  
第 4-1 部分：產品開發要求  
IEC 62443-4-1: Industrial communication networks  
Network and system security  
Part 4-1: Product development requirements
- IEC 62443-4-2：工業通信網路 – 網路與系統安全  
第 4-2 部分：IACS 服務提供者的安全方案要求  
IEC 62443-4-2: Industrial communication networks  
Network and system security  
Part 4-2: Technical security requirements for IACS components
- EDSA-311: ISA 安全嵌入式設備安全保障 – 功能安全性評估  
EDSA-311: ISA Security Compliance Institute Embedded Device Security Assurance Functional Security Assessment
- EDSA-312: ISA 安全嵌入式設備安全保障 – 軟體發展安全性評估  
EDSA-312: ISA Security Compliance Institute Embedded Device Security Assurance Software Development Security Assessment

## 功能安全要求

### FUNCTIONAL SAFETY REQUIREMENTS

產品具備足夠的可靠性和安全性，符合規定相關標準（例如 IEC 61508，EN ISO 13489-1）安全完整性等級 (SIL) 和性能等級 (PL) 要求，適用於安全相關領域，以充分地保護人類和環境。

The products are adequately reliable and safe in accordance with a defined safety level (Safety Integrity Level (SIL), Performance Level (PL) etc.) of the relevant standards (for example IEC 61508, EN ISO 13489-1) and are suitable to be applied in safety related applications in order to protect human beings and the environment sufficiently.

## 資訊安全要求

### SECURITY REQUIREMENTS

在產品開發和整合階段，根據定義的安全級別（安全級別 SL 1 至 SL 4）為產品提供充分保護，防止操縱和干擾。

Sufficient protection against manipulation and interference in accordance with the defined security level (Security Level SL 1 to SL 4) during the development and for the integration phase of products.

## 研討會與公開課

### WORKSHOP AND PUBLIC COURSES

「工業自動化網路安全」主題的研討會和公開課將側重於系統安全性群組件開發。

Our workshop and public courses regarding the topic "Cybersecurity for Industrial Automation" focuses on the development of safety-ensuring components of a system.

一天的研討會將向與會者介紹系統架構，實施和測試的要求規範。

The one day workshop will give participants an overview about the normative requirements to the architecture of a system and its implementation and testing.

三天的公開課程則更詳細：

包括資訊安全相關標準 IEC 62443-3-3，IEC 62443-4-1 和 IEC 62443-4-2 的要求和問題解決方案。同時將介紹並討論功能安全和資訊安全產品開發的全部要求。

The 3-day training will be more detailed:

Standards IEC 62443-3-3, IEC 62443-4-1 and IEC 62443-4-2 will be discussed and solutions shown. All requirements necessary to develop a functional safe and secure product will be presented and discussed.

## 我們的服務承諾

### OUR SERVICES COMMITMENT

- 全球唯一獲得德國 DAkkS 及 ISASecure™ 機構授權，提供一站式集國際功能安全標準、歐洲及美國資訊安全標準進行產品測試和驗證

The only company authorized by German DAkkS and ISASecure™ to provide one-stop set of international functional safety standards, European and American cyber security standards for product testing and certification

- 公開及定制化的研討會和公開課  
Workshops and public courses

- 資訊安全系統及功能安全系統評估  
Assessment and qualification of QM-systems

- 威脅建模，風險分析  
Threat & risk analysis

- 網路安全審核  
Safety audits of networks

- 漏洞掃描  
Vulnerability scans

## 搭建資訊安全管理系統，提升 IT 服務管理水準

# Safeguard the information security and enhance the IT service management

- ISO/IEC 27001 資訊安全管理系統  
ISO/IEC 27001 Information security management system

- ISO/IEC 27017 雲服務資訊安全管理控制實施規範  
ISO/IEC 27017 Information technology - Security techniques - Code of practice for information security controls base on ISO/IEC 27002 for cloud services

- ISO/IEC 27018 公共雲個人資訊 (PII) 處理者的資訊安全控制規範  
ISO/IEC 27018 Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

- ISO/IEC 20000 資訊技術服務管理系統  
ISO/IEC 20000 IT service management system

- VDA-ISA VDA 資訊安全評估 (汽車產業)  
VDA-ISA VDA Information Security Assessment

- TISAX 可信資訊安全評估 (汽車產業)  
TISAX Trusted Information Security Assessment Exchange

- ISO 22301 公共安全業務連續性管理系統  
ISO 22301 Social security-business continuity management systems

# 德國萊因 TÜV 學院與生命關懷：您的網路安全輔導專家

## TÜV Rheinland Academy and Life Care: Cybersecurity courses and consulting services

- GDPR（歐盟通用資料保護條例）法規解析  
GDPR (General Data Protection Regulation) analysis
- 德國萊因 TÜV PersCert 資料保護專員資格課程 \*  
TÜV Rheinland PersCert qualification courses for data protection representative
- 德國萊因 TÜV PersCert 資料保護審核員資格課程  
TÜV Rheinland PersCert qualification courses for data protection auditor
- GDPR 差距分析及系統 / 流程輔導  
GDPR Gap analysis and system/process coaching
- ISO 27001 資訊安全管理系統標準及內審員公開課程  
Public courses for ISO 27001 information security management system standards and internal auditor
- ISO 20000 資訊服務管理系統標準及內審員公開課程  
Public courses for ISO 20000 information technology service management system standards and internal auditor

\*GDPR 法規要求，企業需要任命資料保護專員來保證合規性。

\*The companies should assign data protection specialists to ensure compliance according to GDPR regulations.



文中所提及的內訓、諮詢、課程、輔導相關服務由萊茵技術監護（深圳）有限公司提供並執行。  
All In-house training and consulting services are implemented by TÜV Rheinland (Shenzhen) Co., Ltd.

## 為什麼選擇德國萊因 TÜV ? Why TÜV Rheinland?

- 獨立測試、檢驗、驗證和網路安全服務的全球領先者  
Global leader in independent testing, inspection, certification, and cybersecurity services
- 從業近 20 年，以全面的諮詢和解決方案幫助改善企業的 IT 和網路安全  
Supporting enterprises with comprehensive consulting and solution expertise in IT and cybersecurity for nearly 20 years
- 在全球 59 個國家，擁有超過 20,000 名專業人員  
Employs over 20,000 professionals across 59 countries
- 擁有全球能力最廣泛的智慧設備以及物聯網測試實驗室，並定義了產業的功能與資訊安全標準  
We operate some of the world's broadest smart device and IoT testing labs and define industry standards for functional safety and security

德國萊因TÜV大中華區  
TÜV Rheinland Greater China  
服務熱線 Hotline  
+886 2 21721001 (台灣 Taiwan)  
+852 21921022 (香港 Hong Kong)  
+86 4008831300 (中國大陸 Mainland China)

[www.tuv.com](http://www.tuv.com)

 **TÜVRheinland**<sup>®</sup>  
Precisely Right.