Greater China

Choose certainty.
Add value.

TÜV南德意志集团

基于IEC 62443的工业信息安全

曾胜吾
TÜV南德意志集团大中华区智能电网经理

TÜV 南德意志集团正在日益壮大

1	一站式技术解决供应商
150	150年的悠久历史
850	850个全球分支机构
2,220	2015年创造了约22.2亿欧元销售额
24,000	全球24,000名员工

Note: Figures have been rounded off.
*As of 29.02.2016: Inclusive of acquisition in January 2016.

专业技术背景和广泛的行业知识

测试和产品认证
化学、物理、机械、电气和环境测试及产品认证。

检验
产品、体系、建筑、工厂、基础设施检验。

审核和体系认证
体系认证渗透到到各个领域，其中包括质量、安全、能源、社会责任和环境。

知识服务
安全、质量、风险、环境保护和监管咨询。

培训
培训包括工作安全、技术能力、管理体系、项目执行。

TÜV 南德意志集团的认证标志和证书是您最优的营销工具

TÜV 南德意志集团这个品牌是质量和安全的代名词。

我们的产品证书是您市场准入的有效工具；我们的测试报告能够使您自信地告诉客户您的产品是安全、高质量和可持续发展的；我们颁发的个人资质证书助您赢得更多的市场良机。

> 500,000 产品证书

> 54,000 体系证书

> 20,000 个人资质证书
> 160,000 受训人员

全球技术，本地经验

图例说明：

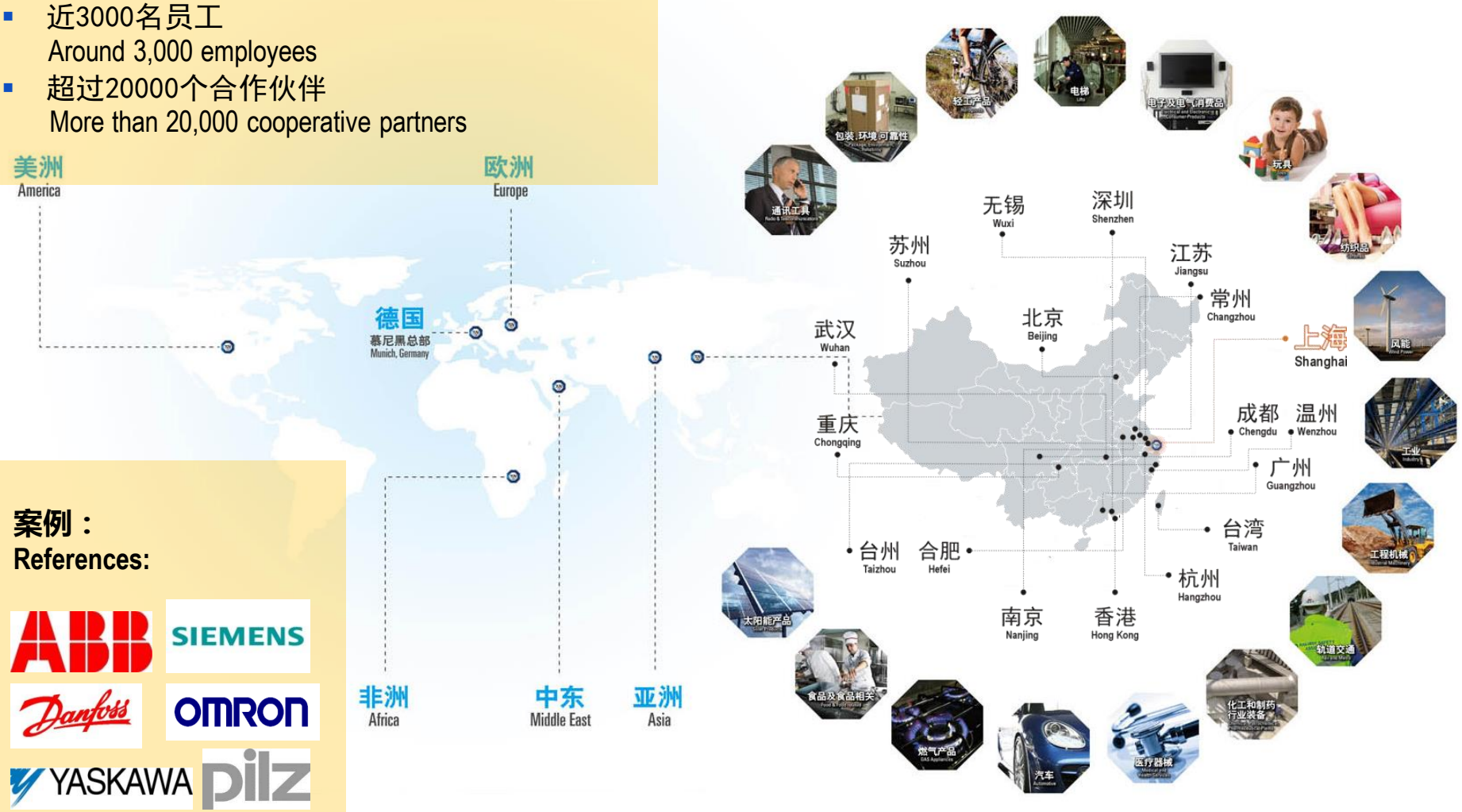
- TÜV 南德意志集团分布的区域
- 各区域的总部

注：以上数据更新至2015年12月31日

德国	国际
12.83亿欧元销售额 11,600 名员工	9.39亿欧元销售额 10,800 名员工

TÜV 南德意志集团大中华区

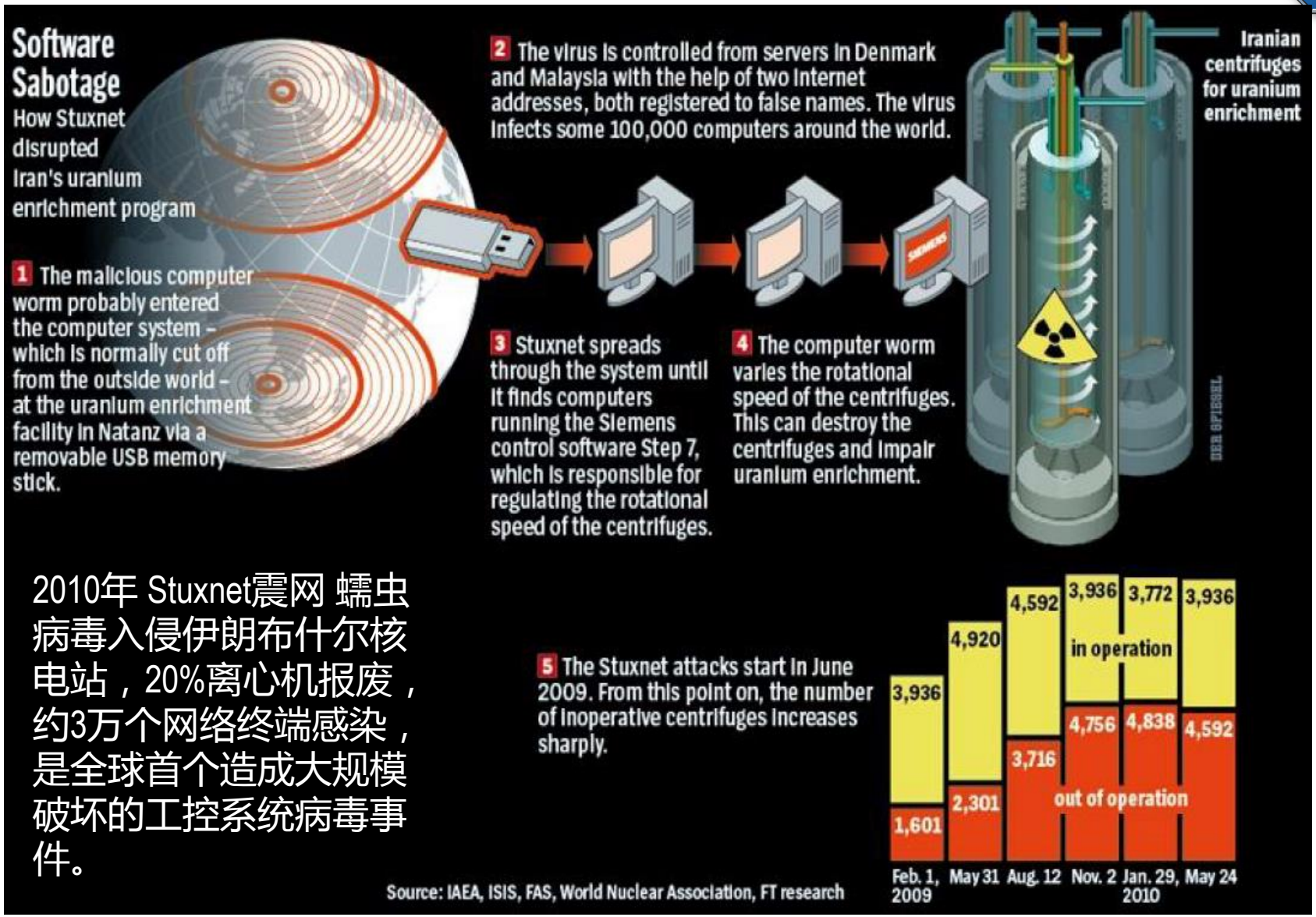
- 全国有超过40个分支机构
  More than 40 offices across China
- 近3000名员工
  Around 3,000 employees
- 超过20000个合作伙伴
  More than 20,000 cooperative partners



案例：
References:

ABB SIEMENS Danfoss OMRON YASKAWA pilz

震网病毒 – 全球首个以工控系统为攻击目标的病毒



2010年 Stuxnet震网 蠕虫病毒入侵伊朗布什尔核电站，20%离心机报废，约3万个网络终端感染，是全球首个造成大规模破坏的工控系统病毒事件。

乌克兰电网攻击事件 – 全球首起黑客攻击造成电网大规模停电

2015年12月23日发生的由木马攻击引起的乌克兰电网电力中断，这是首次由恶意软件攻击导致国家基础设施瘫痪的事件，致使乌克兰城市伊万诺弗兰科夫斯克将近一半的家庭（约140万人）在2015年圣诞节前夕经历了数小时的电力瘫痪。

信息安全的三大基本要素 – CIA

Confidentiality	• **保密性** • 信息不被泄露给非授权的用户，实体或过程
Integrity	• **完整性** • 数据不被篡改，破坏或丢失
Availability	• **可用性** • 系统功能正常运行

工业信息安全 与 IT信息安全 – 基本要求不同

工业自动化控制系统的信息安全的基本要求，与传统的IT信息安全侧重不同

通用信息系统 (IT)	重要性	工业自动化控制系统 (OT)
保密性	↑	可用性
完整性		完整性
可用性		保密性

办公自动化
ERP
财务系统
人力

调度自动化
变电站自动化
监控系统
厂站自动化
轨道交通
过程控制
航空航天

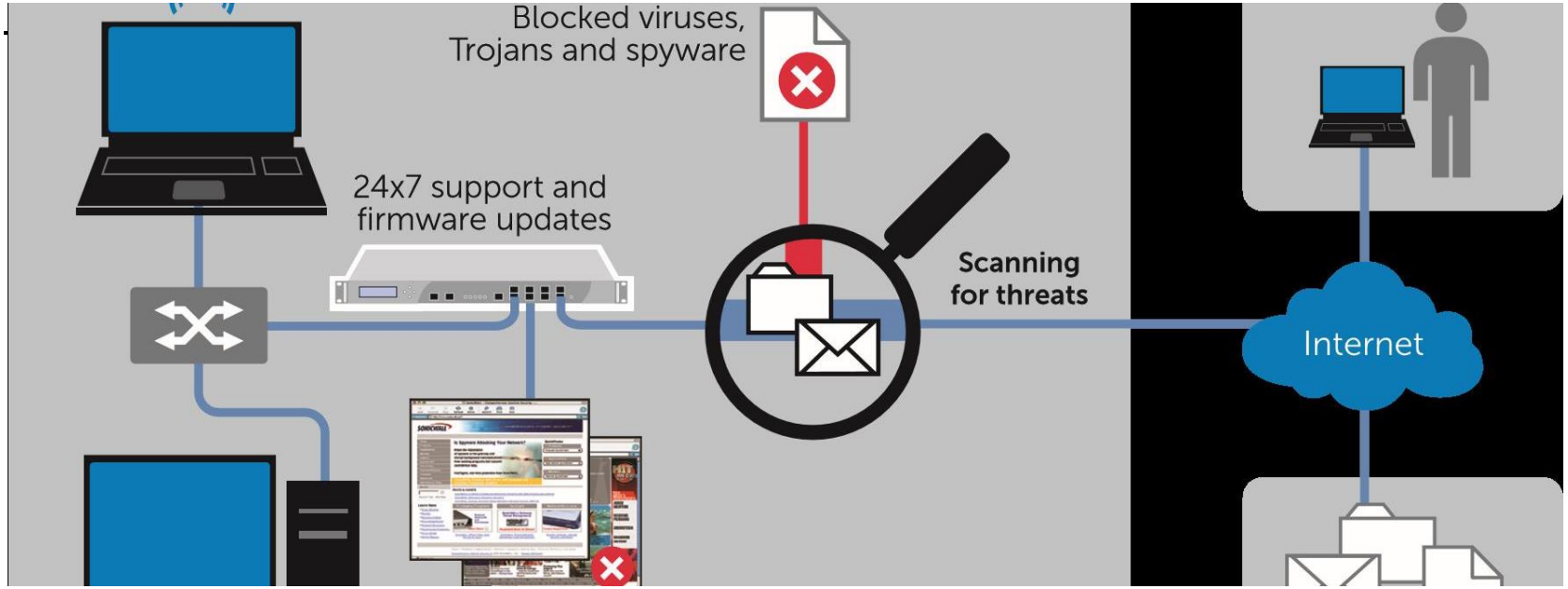
信息安全的**产品**

- 产品通过测试 ≠ 产品的信息安全
  - 今天测试安全的产品，无法发现所有将来可能出现的新漏洞，与相对应的攻击手段
  - IEC 62443-2-3 Patch management
  - IEC 62443-4-1 Practice 7 – Security Update Management
    - PM-1: Security Update Qualification
    - PM-2: Security Update Documentation
    - PM-3: Dependent Component or Operating System Security Update Documentation
    - PM-4: Security Update Delivery
    - PM-5: Timely Delivery of Security Patches

Industrial **C**ontrol **S**ystems – **C**yber **E**mergency **R**esponse **T**eam 工控系统网络威胁应急小组

信息安全的**系统**

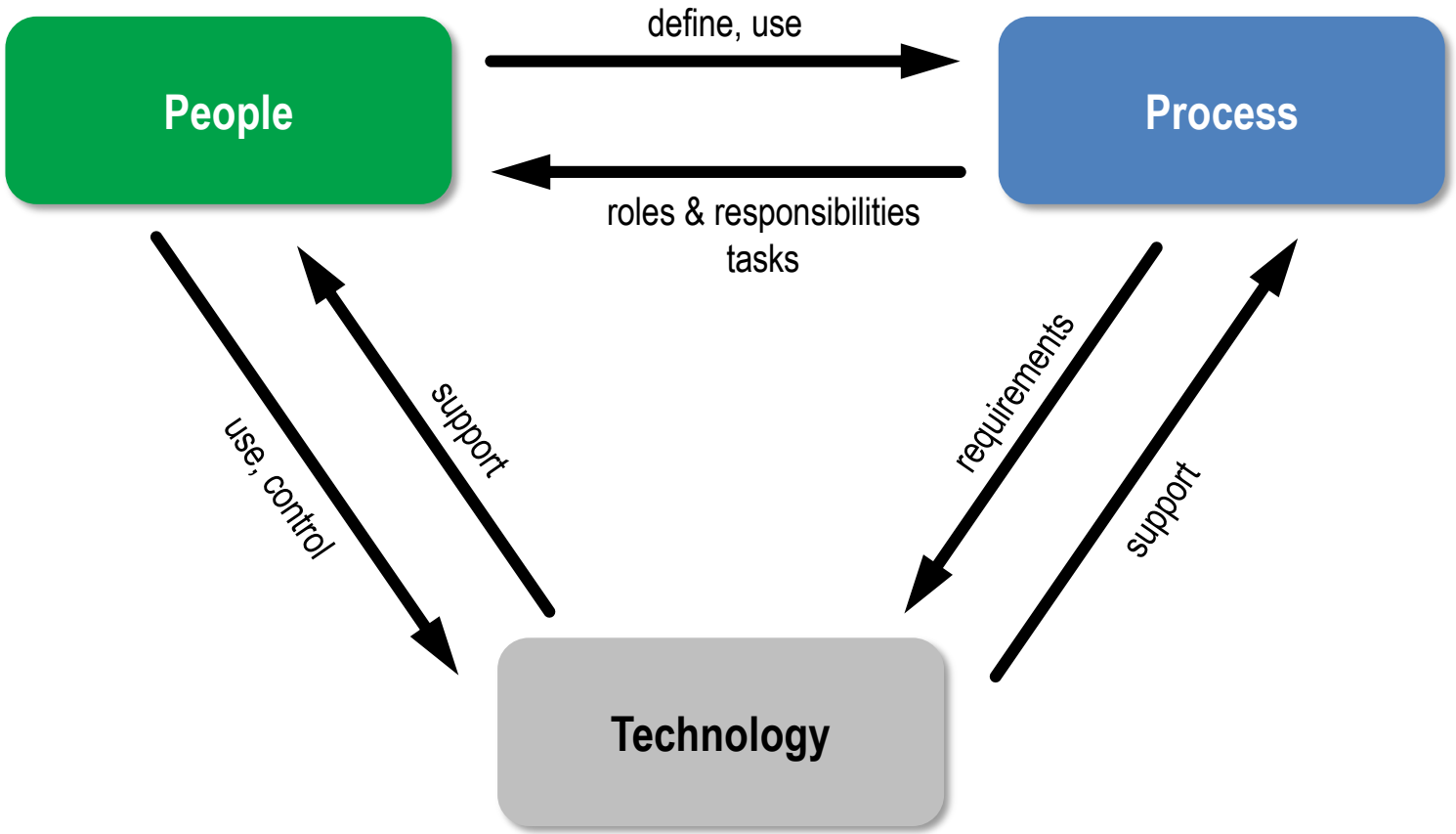
- 信息安全的产品 ≠ 信息安全的系统
  - 不合理的配置（相应安全功能未启用，错误的产品搭配，不合理的系统设计等）会导致由安全的产品构成的系统不安全
  - IEC 62443-3-3:
    - 7个基本要求（抽象）
    - 53个系统要求（具体）
  - E.g. FR1, SR 1.1 RE 1 – Unique identification and authentication



信息安全的**运营**

- 信息安全的系统 ≠ 信息安全
  - 运行人员密码泄露，维护人员电脑带毒，信息安全操作流程未落实…
  - IEC 62443-2-1: 工控系统如何正确的操作，维护，拆毁….

People, Process, Technology



信息安全 – 短板效应

- 系统中最薄弱的一环，决定了系统的安全程度

IEC 62443 – 工业通信网络 信息安全

IEC 62443

Industrial communication networks – Network and system security

General	Policies & Procedures	System	Component / Product
1-1 Terminology, concepts and models	2-1 Requirements for an IACS security management system	3-1 Security technologies for IACS	4-1 Secure Product Development Lifecycle Requirements
1-2 Master glossary of terms and abbreviations	2-2 Implementation guidan-ce for an IACS security management system	3-2 Security Risk Assessment and System Design	4-2 Technical security requirements for IACS components
1-3 System security compliance metrics	2-3 Patch management in the IACS environment	3-3 System security requirements and security levels	
1-4 IACS security lifecycle and use-case	2-4 Security program requirements for IACS service providers		

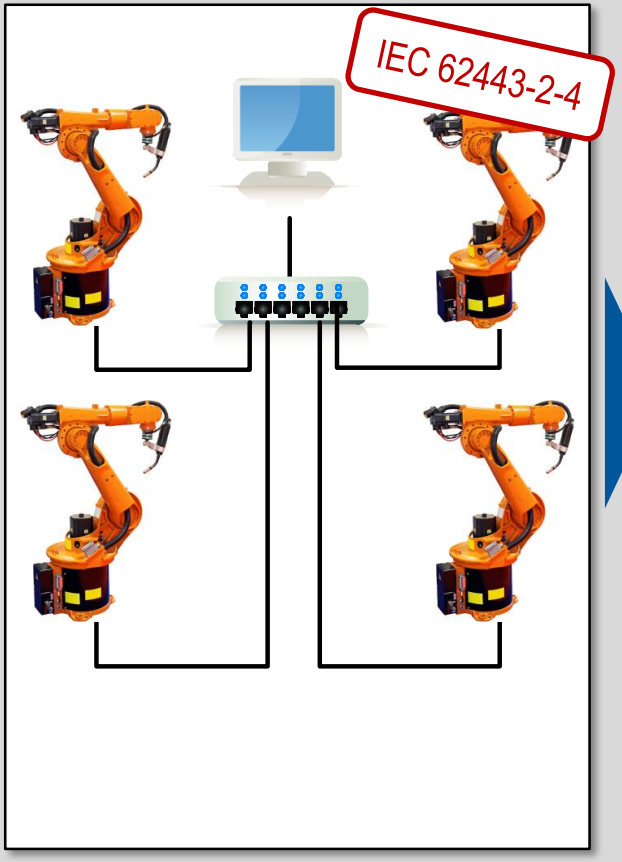
已发布

IEC 草案通过

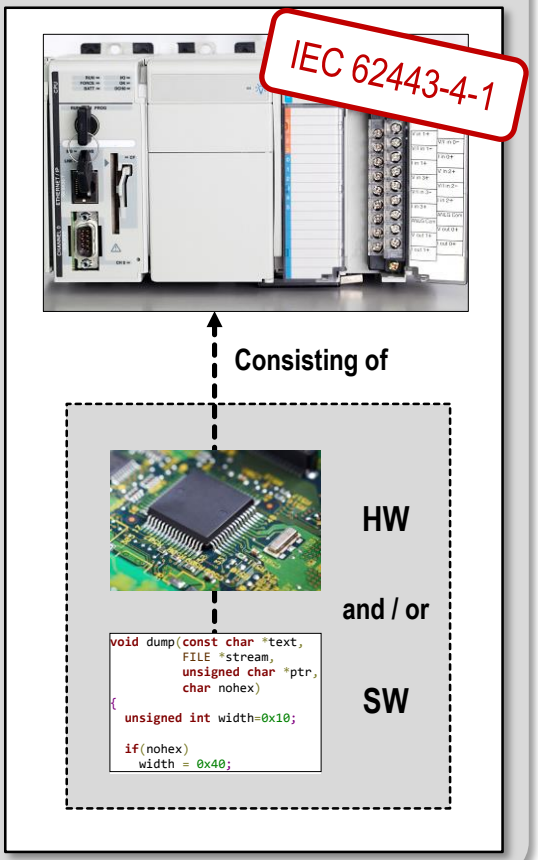
IEC 62443 适用范围示例：生产线

用户
IACS (System)

系统集成商
Automation Solution



设备厂家
Control System / Product



IEC 62443 工业信息安全的7个(维度的)基本要求

Foundational Requirements (FRs)

"A small set of Foundational Requirements shall be used to derive the full scope of detailed Technical and Program Requirements."

IEC 62443定义了工业自动化系统 信息安全的7个方面的基本要求

- **身份和授权控制 Identification & Authentication Control (IAC)**
- **使用控制 Use Control (UC)**
- **系统完整性 System Integrity (SI)**
- **数据保密性 Data Confidentiality (DC)**
- **受限数据流 Restricted Data Flow (RDF)**
- **事件的实时响应 Timely Response to Events (TRE)**
- **资源可用性 Resource Availability (RA)**

General Concepts of IEC 62443: Security Levels

Security Level 安全等级

“衡量工业自动化系统抵御恶意攻击的能力”

IEC 62443定义的4个安全等级:

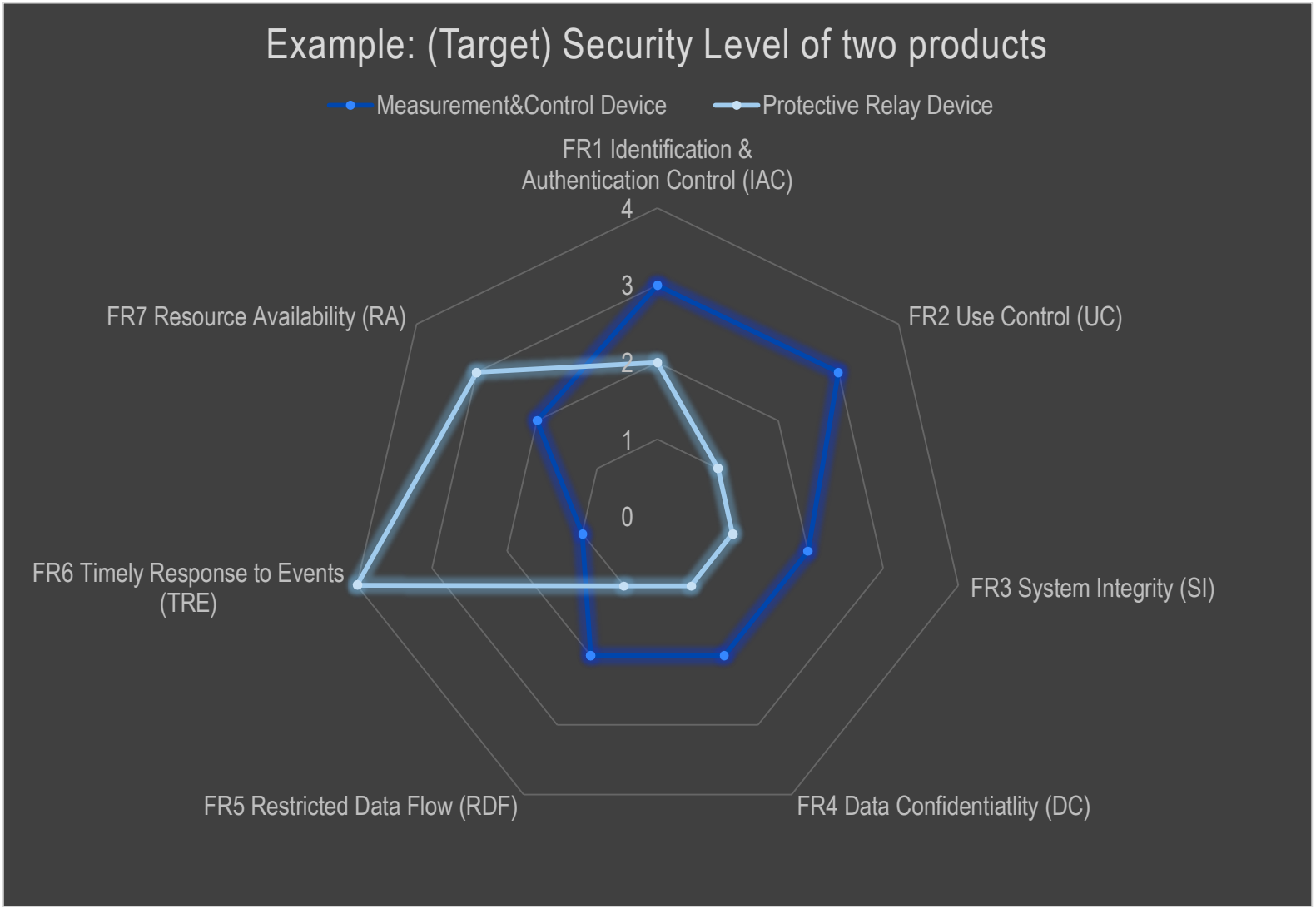
SL	攻击手段	资源	技术	动机
1	偶然的或巧合的			
2	简单	低	通用的	低
3	复杂	中等	特定系统专有	中等
4	复杂	大规模	特定系统专有	强烈

IEC 62443 系统要求 与 安全级别的映射(示例)

	SL1	SL2	SL3	SL4
FR 1 – Identification and Authentication Control (IAC)				
SR 1.1 – Human user identification and authentication	**X**	**X**	**X**	**X**
The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.				
RE (1) Unique identification and authentication		**X**	**X**	**X**
The control system shall provide the capability to uniquely identify and authenticate all human users.				
RE (2) Multifactor authentication for untrusted networks			**X**	**X**
The control system shall provide the capability to employ multifactor authentication for human user access to the control system via an untrusted network (see 4.14, SR 1.12 – Access via untrusted networks).				
RE (3) Multifactor authentication for all networks				**X**
The control system shall provide the capability to employ multifactor authentication for all human user access to the control system.				

安全等级是一个七维向量！Security Level is a vector !

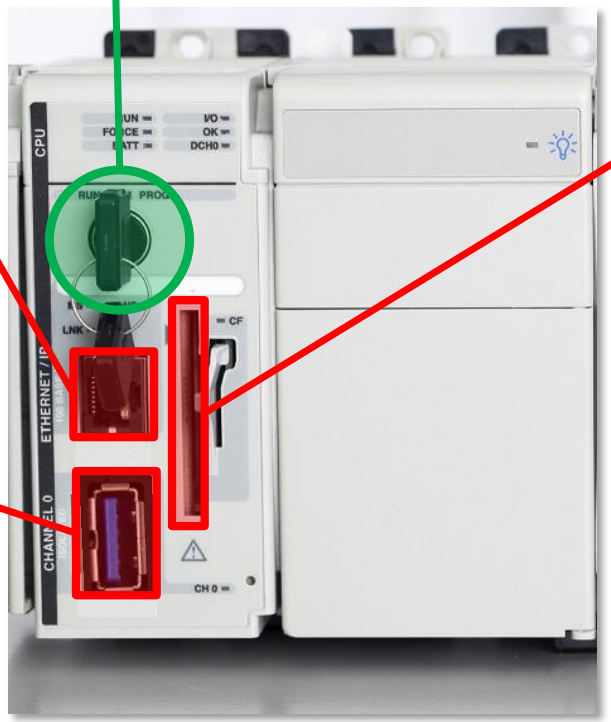
Security Level = （ FR1, FR2, FR3, FR4, FR5, FR6, FR7 ）



Product Supplier (Example: PLC)

Keylock

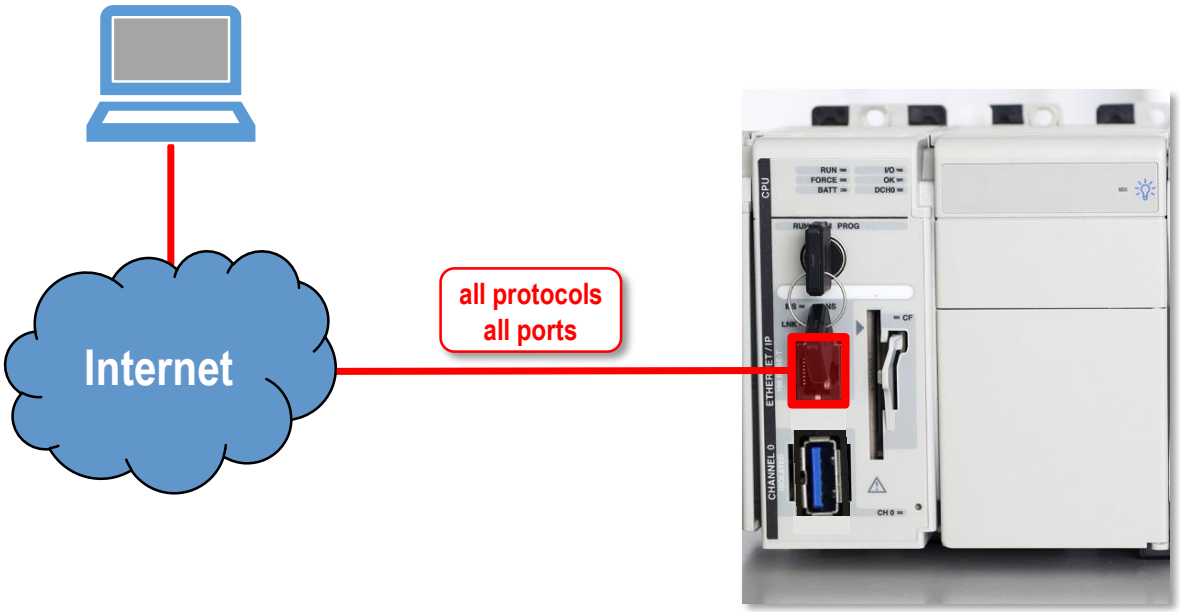
Ethernet:
- Network access



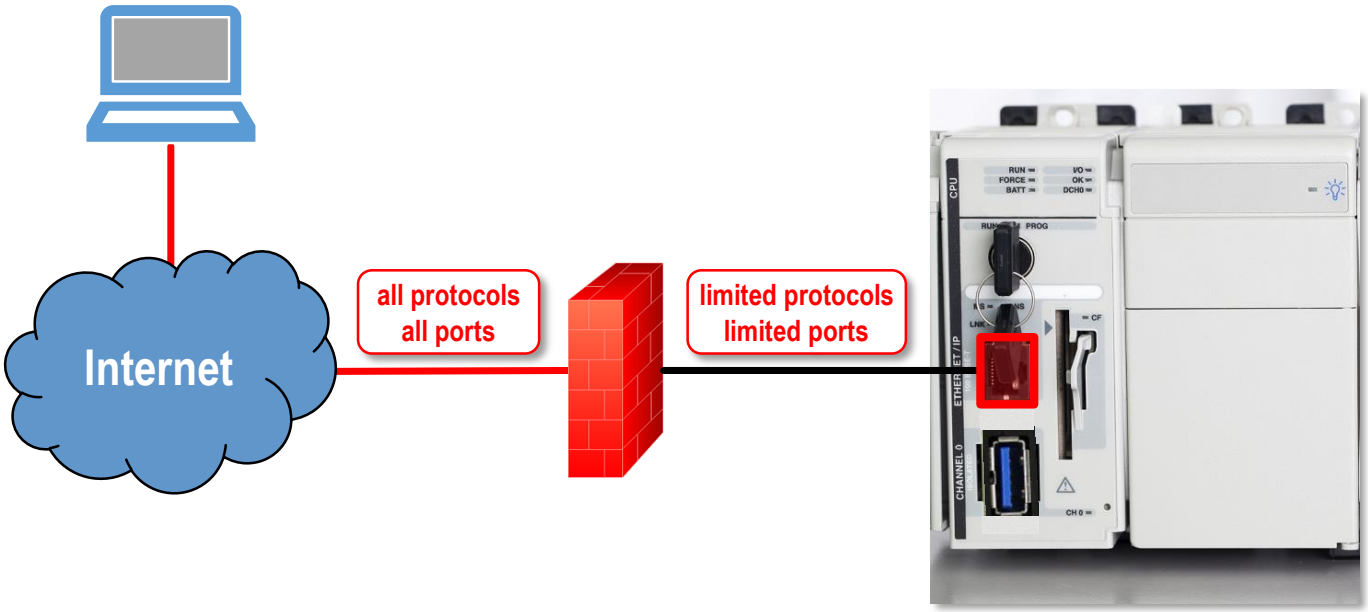
SD-Card:
- Software / Firmware Image
- Code Signing
- Physical Access Control

USB Port
- Application
- Parameters
- Engineering Data
- …
- Authentication
- Encryption
- Digital Signatures
- Physical Access Control

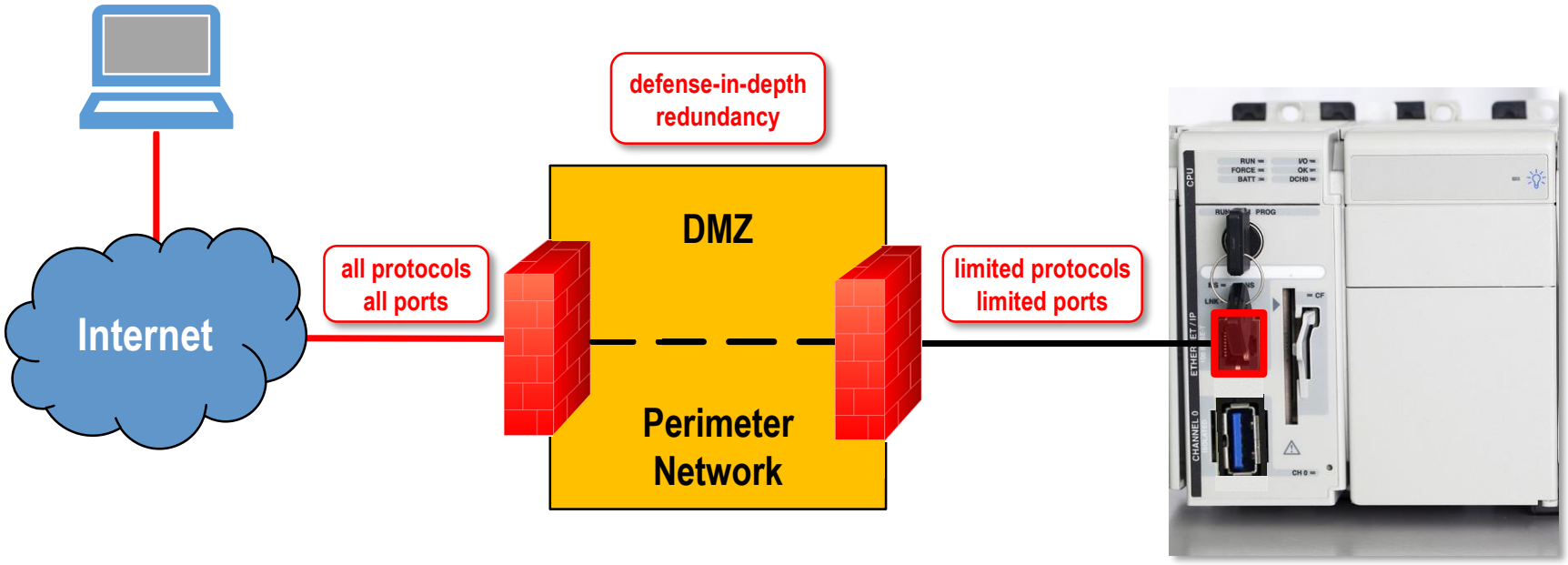
Product Supplier (Example: PLC) – Scenario 1



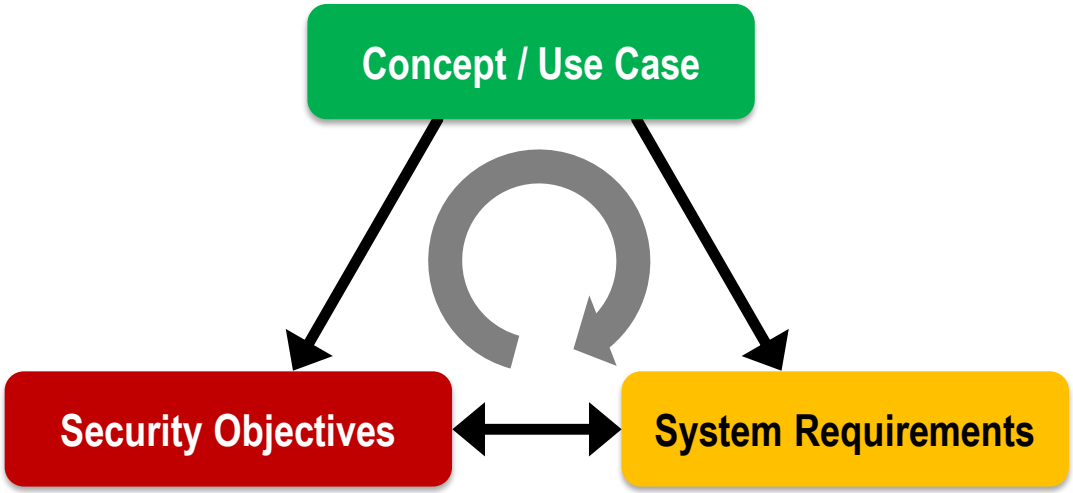
Product Supplier (Example: PLC) – Scenario 2



Product Supplier (Example: PLC) – Scenario 3



Example: V-Model



项目案例: 西门子全球首批TÜV 南德IEC 62443认证

近日2016年8月，西门子成为首家在TUV南德取得基于IEC 62443工业信息安全认证的厂家。

其中，西门子工业集团的**工控系统及组件PCS7**获得产品认证，西门子能源集团获得得**变电站自动化解决方案**认证 。

截止2017年8月，西门子共有**18个研发及制造中心**获得基于通用的产品全生命周期研发管理流程的认证。

项目案例: 西门子全球首批TÜV 南德IEC 62443认证

ZERTIFIKAT ◆ CERTIFICATE ◆ 認証書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Product Service

CERTIFICATE

No. Z2 16 10 67801 001

Holder of Certificate: Siemens AG
PD PA AE
Östliche Rheinbrückenstr. 50
76187 Karlsruhe
GERMANY

Production Facility(ies): 67801

Certification Mark:

Product: Industrial Control Systems and Components

Model(s): SIMATIC PCS 7

Parameters: Process Control System

Tested according to: PPP 50156B:2016
(based on IEC 62443-4-1)
IEC 62443-3-3(ed.1)

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: SK90104C

Valid until: 2019-10-20

Date, 2016-10-21 (Christian Dimeier)

Page 1 of 1

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstraße 65 · 80339 München · Germany

TÜV®

认证企业

- **西门子 (作为设备厂家)**

认证对象

工控自动化系列产品

- SIMATIC PCS 7

参照标准

- IEC 62443-4-1
- IEC 62443-3-3 (will use -4-2 when released)

TÜV 南德 工业信息安全 产品认证 相关标准

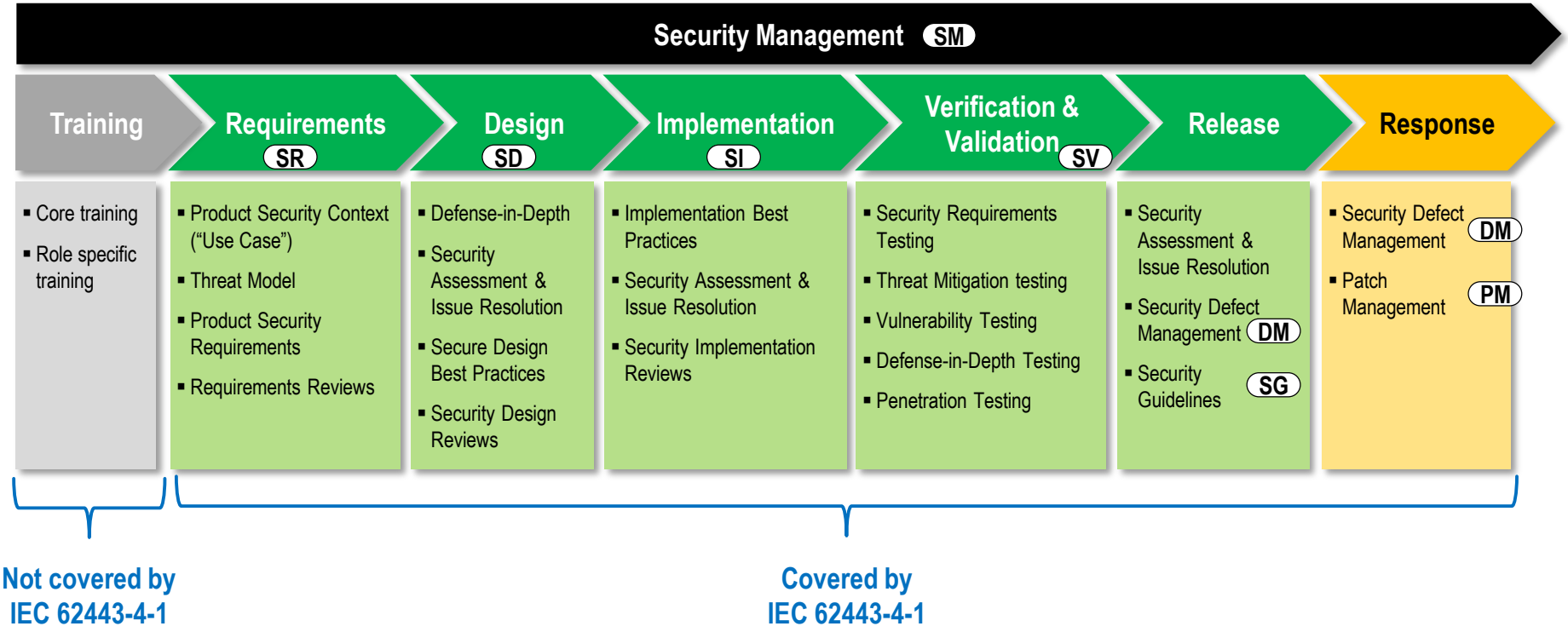
IEC 62443

Industrial communication networks – Network and system security

General	Policies & Procedures	System	Component / Product
1-1 Terminology, concepts and models	2-1 Requirements for an IACS security management system	3-1 Security technologies for IACS	**4-1 Secure Product Development Lifecycle Requirements**
1-2 Master glossary of terms and abbreviations	2-2 Implementation guidance for an IACS security management system	3-2 Security Risk Assessment and System Design	4-2 Technical security requirements for IACS components
1-3 System security compliance metrics	2-3 Patch management in the IACS environment	**3-3 System security requirements and security levels**	
1-4 IACS security lifecycle and use-case	2-4 Security program requirements for IACS service providers		

Basis for Certification

IEC 62443-4-1: Secured Product Development Life Cycle (SPDLC)



IEC 62443-4-1: 安全的产品开发流程 (SPDLC)

- **SPDLC consists of 8 practices （8个最佳实践）**
  - 安全管理 Security Management (SM) — **How is the product being developed?**
  - 安全需求规范 Security Requirements Specification (SR)
  - 纵深防御 Defense-in-depth Strategy (SD)
  - 安全实现 Secure Implementation (SI)

  — **What product is being developed?**
  - 安全验证 Security Verification & Validation (SV) — **Is the product working as designed / specified?**
  - 缺陷管理 Security Defect Management (DM) — **How are product security-related issues identified and handled?**
  - 补丁管理 Patch Management (PM) — **How are patches / fixes provided?**
  - 安全导则 Security Guidelines (SG) — **How to integrate, configure & maintain?**

项目案例: 西门子全球首批TÜV 南德IEC 62443认证

ZERTIFIKAT ◆ CERTIFICATE ◆ 認証書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD Product Service

CERTIFICATE

No. Q4B 17 08 76903 002

Holder of Certificate: Siemens AG
DF TI QM
Östliche Rheinbrückenstr. 50
76187 Karlsruhe
GERMANY

Certification Mark:

Scope of Certificate: Secure Product Development LifeCycle - Product Lifecycle Management Reference Process for Division of Digital Factory (DF) and Process Industries and Drives (PD)

The Certification Body of TÜV SÜD Product Service GmbH certifies that the company mentioned above has established and is maintaining a management system which meets the requirements of the listed standards. The results are documented in a report. See also notes overleaf.

Report No.: SK89768C

Valid until: 2020-08-30

Date, 2017-08-31 (Christian Dirmeier)

Page 1 of 2

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstraße 65 · 80339 München · Germany

TÜV®

认证企业

- **西门子 (作为设备厂家) 德国18个研发制造中心**

认证对象

通用的产品全生命周期研发管理流程

- Secure Product Development LifeCycle

参照标准

- IEC 62443-4-1
- IEC 62443-3-3 (will use -4-2 when released)

项目案例: 西门子全球首批TÜV 南德IEC 62443认证

ZERTIFIKAT ◆ CERTIFICATE ◆ 認証証書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Product Service

CERTIFICATE

No. Z2 16 10 62845 001

Holder of Certificate: Siemens AG
EM DG SYS
Humboldtstraße 59
90459 Nürnberg
GERMANY

Production Facility(ies): 62845

Certification Mark:

Product: Industrial Control Systems and Components

Model(s): Secure Substation Automation Solution

Parameters:

Substation Automation Controller:	Siemens SICAM PAS/PQS; SICAM AK 3
Human Machine Interface (HMI):	Siemens SICAM SCC
Protection Devices:	Siemens SIPROTEC 5
Router/Firewall:	Siemens RUGGEDCOM
Switches:	Siemens RUGGEDCOM
Time Server and Service PC	

Tested according to: IEC 62443-2-4(ed.1)
IEC 62443-3-3(ed.1)

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: SN90105C

Valid until: 2019-10-23

Date, 2016-10-24

(Christian Dirmeier)

Page 1 of 1

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstraße 65 · 80339 München · Germany

TÜV

认证企业

- 西门子 (作为系统集成商)

认证对象

信息安全的变电站自动化系统，包含以下典型设备

- 变电站自动化装置 SICAM PAS/PQS, AK3
- 人机界面 SICAM SCC
- 继电保护 SIPROTEC 5
- 路由器/防火墙 RUGGEDCOM
- 交换机 RUGGEDCOM

参照标准

- IEC 62443-2-4
- IEC 62443-3-3

TÜV 南德 工业信息安全 产品认证 相关标准

IEC 62443

Industrial communication networks – Network and system security

General	Policies & Procedures	System	Component / Product
1-1 Terminology, concepts and models	2-1 Requirements for an IACS security management system	3-1 Security technologies for IACS	4-1 Secure Product Development Lifecycle Requirements
1-2 Master glossary of terms and abbreviations	2-2 Implementation guidance for an IACS security management system	3-2 Security Risk Assessment and System Design	4-2 Technical security requirements for IACS components
1-3 System security compliance metrics	2-3 Patch management in the IACS environment	**3-3 System security requirements and security levels**	
1-4 IACS security lifecycle and use-case	**2-4 Security program requirements for IACS service providers**		

Basis for Certification

IEC 62443-2-4 对系统集成商的要求

Maturity Level 成熟度

“衡量系统集成商在系统集成，维护等活动中满足安全需求的能力”

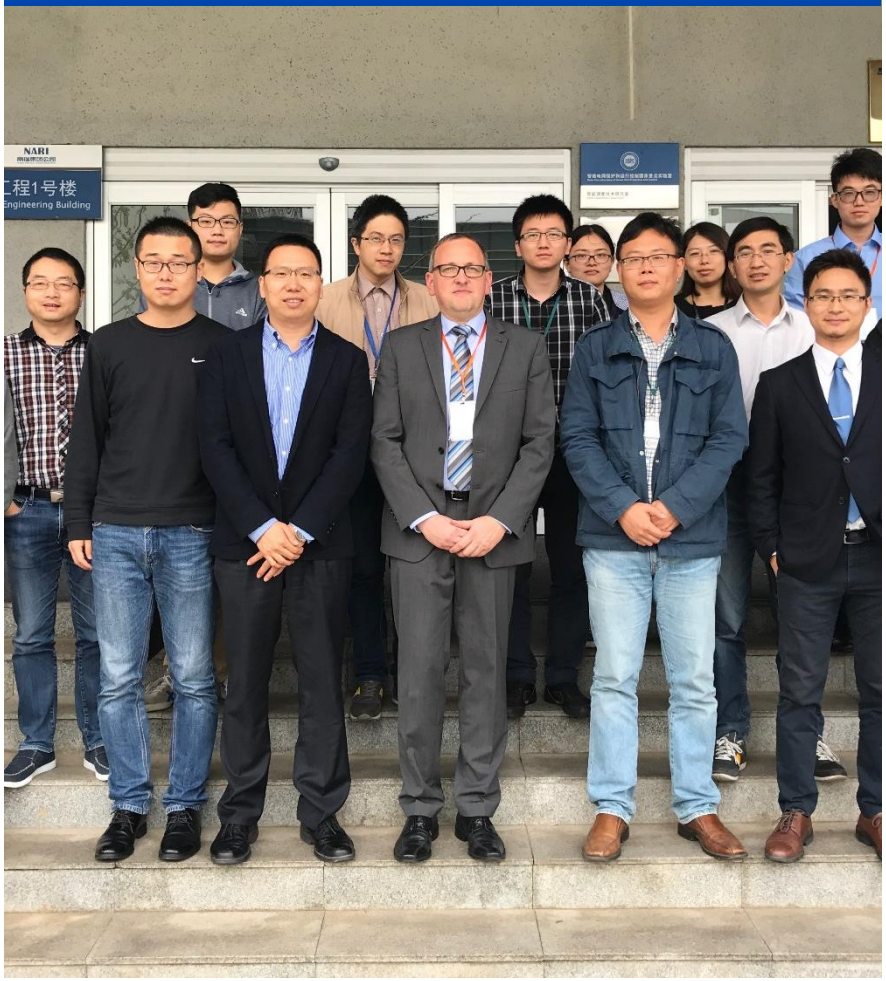
IEC 62443定义的4个系统集成商成熟度:

- **Level 1: 初级**
  无计划的，或者无文件记录的
- **Level 2: 受控**
  有书面政策，个人能力，书面的流程
- **Level 3: 精通**
  多次跨组织的实践
- **Level 4: 改进**
  基于技术，流程，管理的持续改进

IEC 62443-2-4定义了**12个功能类别**

项目案例: 南瑞集团 IEC 62443定制培训

IEC 62443培训及差距分析， 南京



项目描述

- 南瑞集团的D5000调度系统是国内应用最广泛的电力调度系统，在出口海外的过程中，海外买家越来越多的提到工业信息安全认证的需求

服务说明

- 为期一周的定制化培训及差距分析

项目产出

- 20+ 信息安全工程师
- 差距分析报告
- 信息安全开发路线图

Market Promotion

- Industrial Cyber Security Open Training, Shanghai, 2017-05-04

Market Promotion

- Industrial Cyber Security Open Training, Guangzhou, 2017-07-27

Market promotion

- Open Training, Singapore, 2017-08-29

Market Promotion – lighthouse, Shanghai, 2017-11-09

参会名单（拟）

机构与协会

工业控制系统信息安全产业联盟、工信部五所、工信部一所
国网浙江省电力公司电力科学研究院、全国工程过程测量和控制标准化技术委员会
工业4.0俱乐部、上海市机器人协会
沈阳自动化所、自动化仪表所、国家工业信息安全产业发展联盟
中国机电一体化技术应用协会

高校

香港科技大学、同济大学、交通大学、复旦大学、浙江大学

企业

ABB、西门子、Honeywell、Rockwell、和利时、QNX、菲尼克斯、施耐德电、GE、浙江中控、北京四方、南瑞集团、南瑞继保、国电南自、许继、Proove AB、CSA集团、Jebsen、国家电网、南方电网、中石化、中石油、发那科、库卡、新松机器人、富士康青岛科捷自动化有限公司、博世中国、奔驰、宝马、奥迪、上汽集团、比亚迪、吉利、长安、东风日产

咨询与金融机构

罗兰贝格、柯力士信息安全、北京威努特技术、北京匡恩网络科技

*以上议程与参会名单均以当天活动为准

Choose certainty.
Add value.

联系方式

曾胜吾

shengwu.zeng@tuv-sud.cn

186 1670 6543