工业信息安全标准IEC 62443的应用与认证

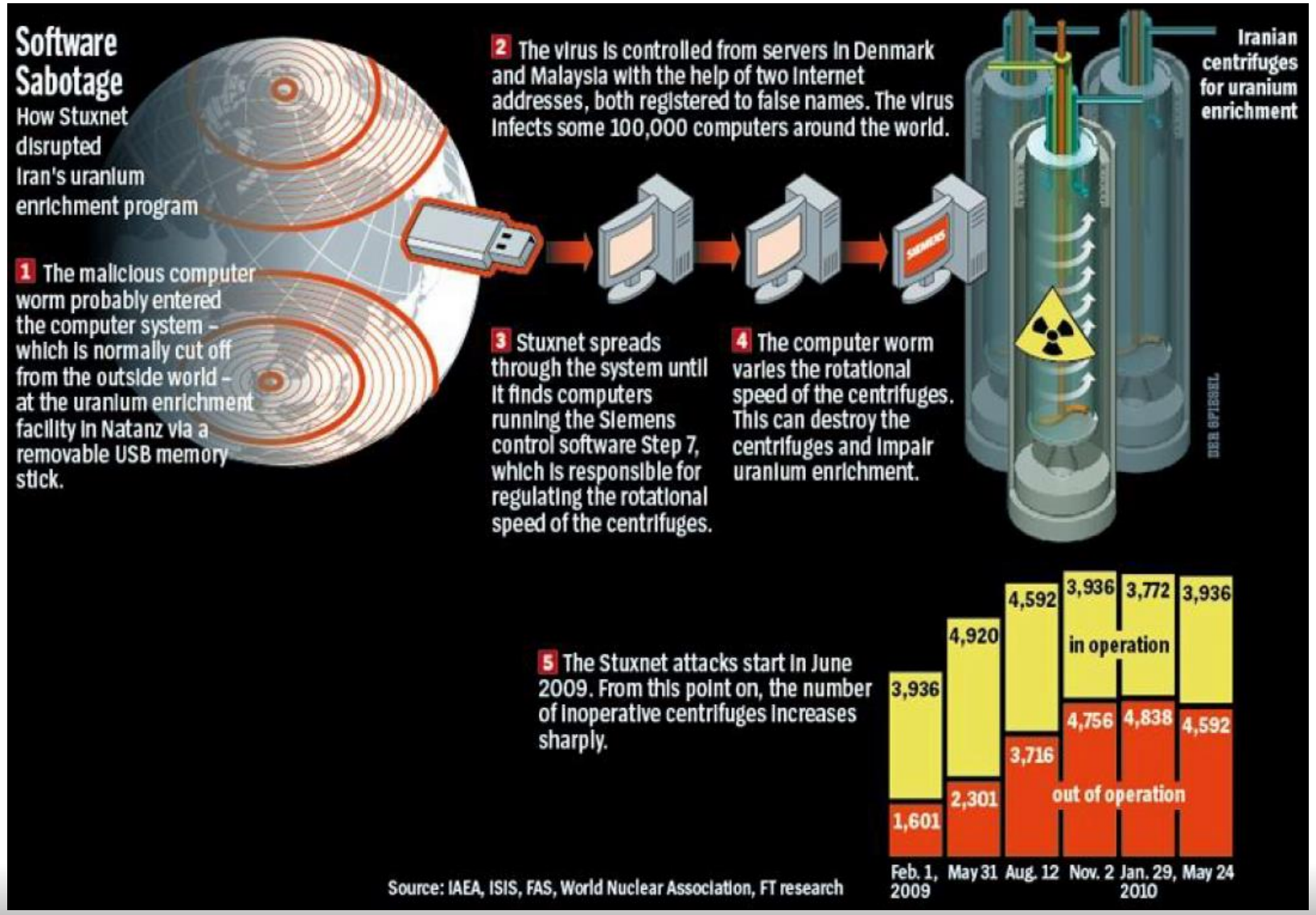
陈荻川
南德认证检测(中国)有限公司
上海分公司

Mehr Wert.
Mehr Vertrauen.

Add value.
Inspire trust.

目录

震网病毒



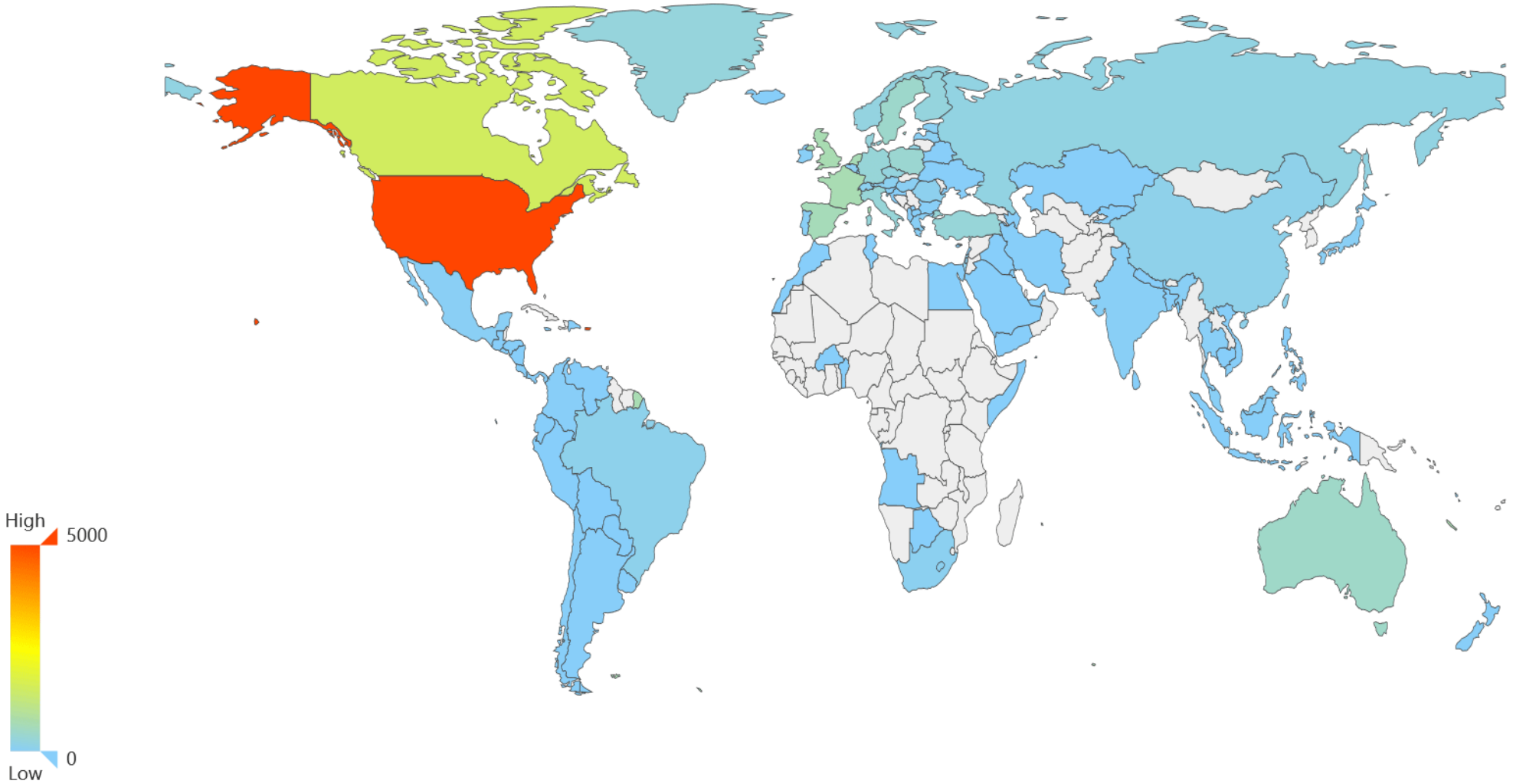
世界上第一例针对工控系统的病毒。

乌克兰电网攻击事件

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。

世界上第一次经证实的网络恶意攻击导致的停电事件

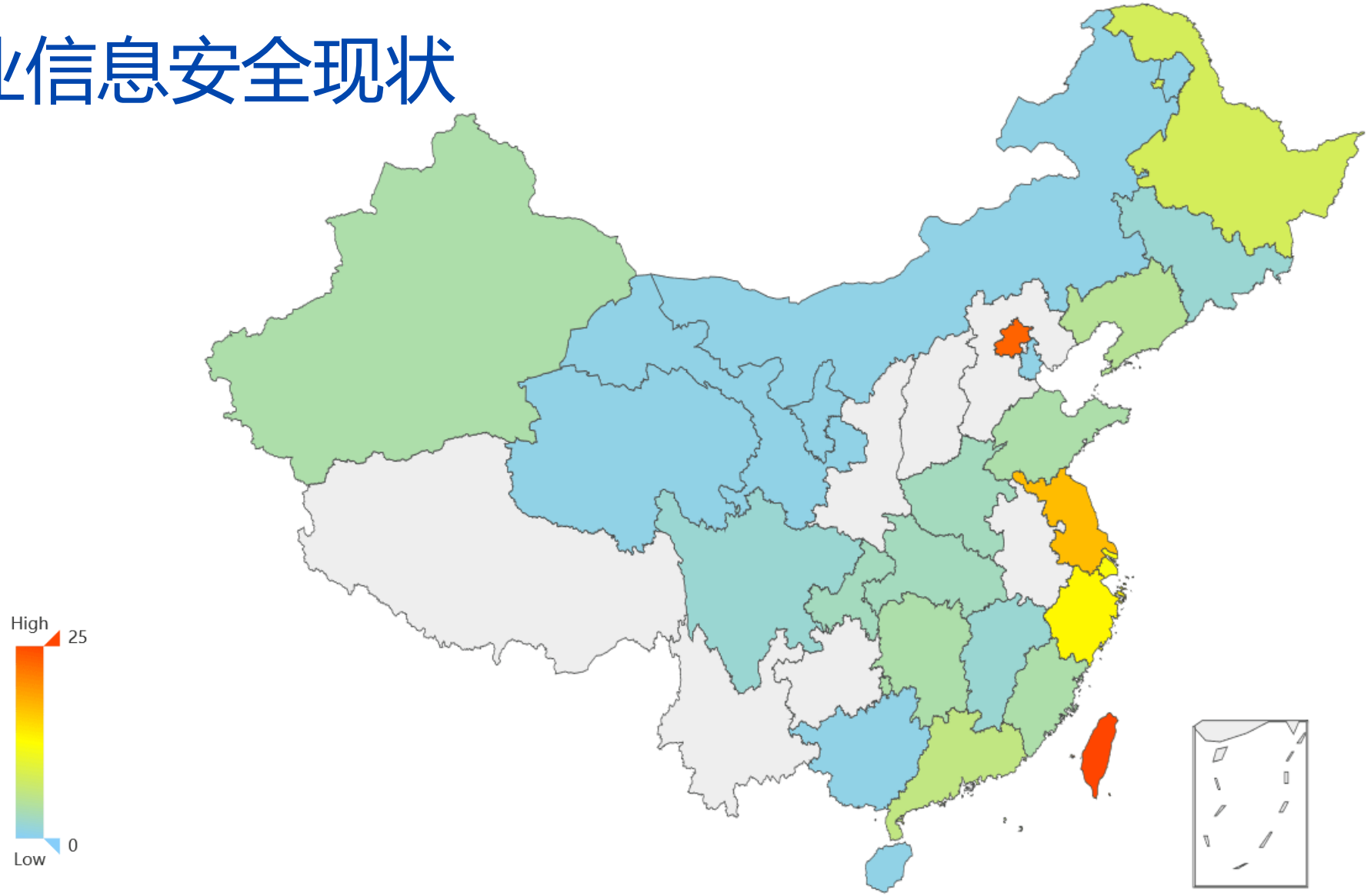
工业信息安全现状



全球工控系统暴露分布图

数据来源：东北大学工控信息安全团队

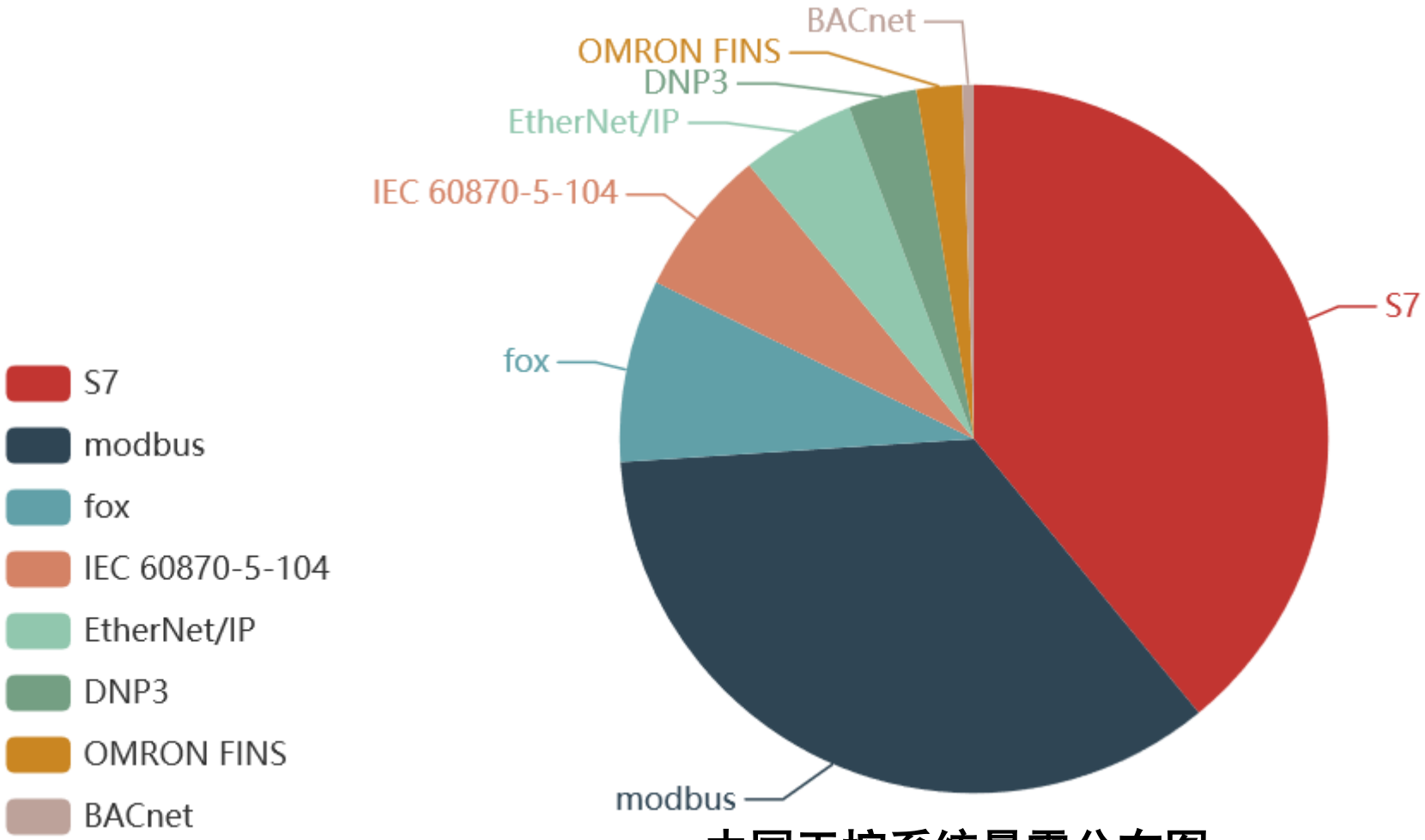
工业信息安全现状



中国工控系统暴露分布图

数据来源：东北大学工控信息安全团队

工业信息安全现状



中国工控系统暴露分布图

数据来源：东北大学工控信息安全团队

工业信息安全现状

美国ICS-CERT历年公布漏洞数

目录

信息安全要解决什么问题?

C **Confidentiality** **保密性**

- 信息不被泄露给非授权的用户，实体或过程

I **Integrity** **完整性**

- 系统和数据，不被破坏、篡改、劫持

A **Availability** **可用性**

- 系统功能正常运行

信息安全的三大基本目标 – C I A

工业控制系统与IT信息系统

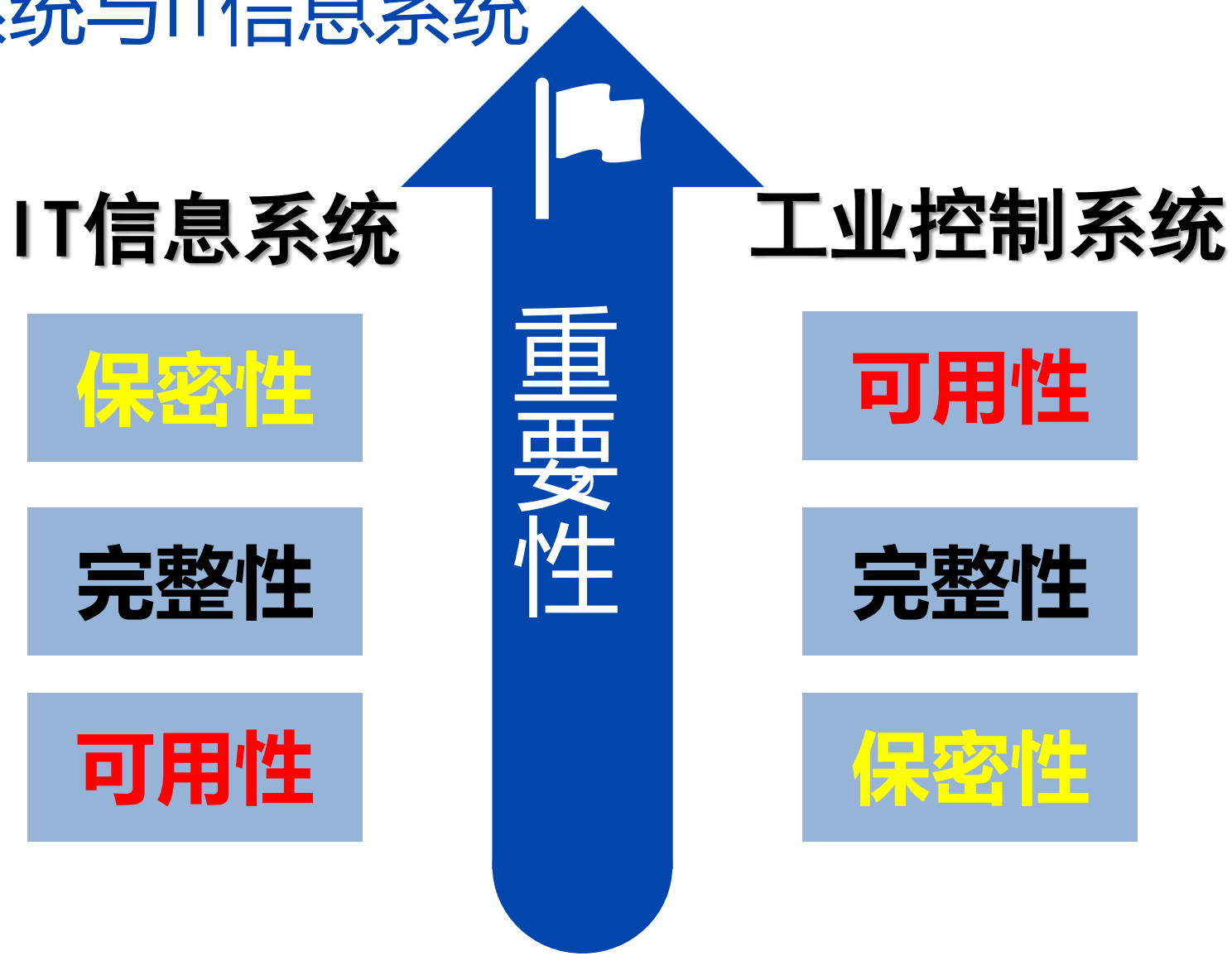
IT信息系统

- 财务系统
- ERP
- 办公自动化
- 网站系统

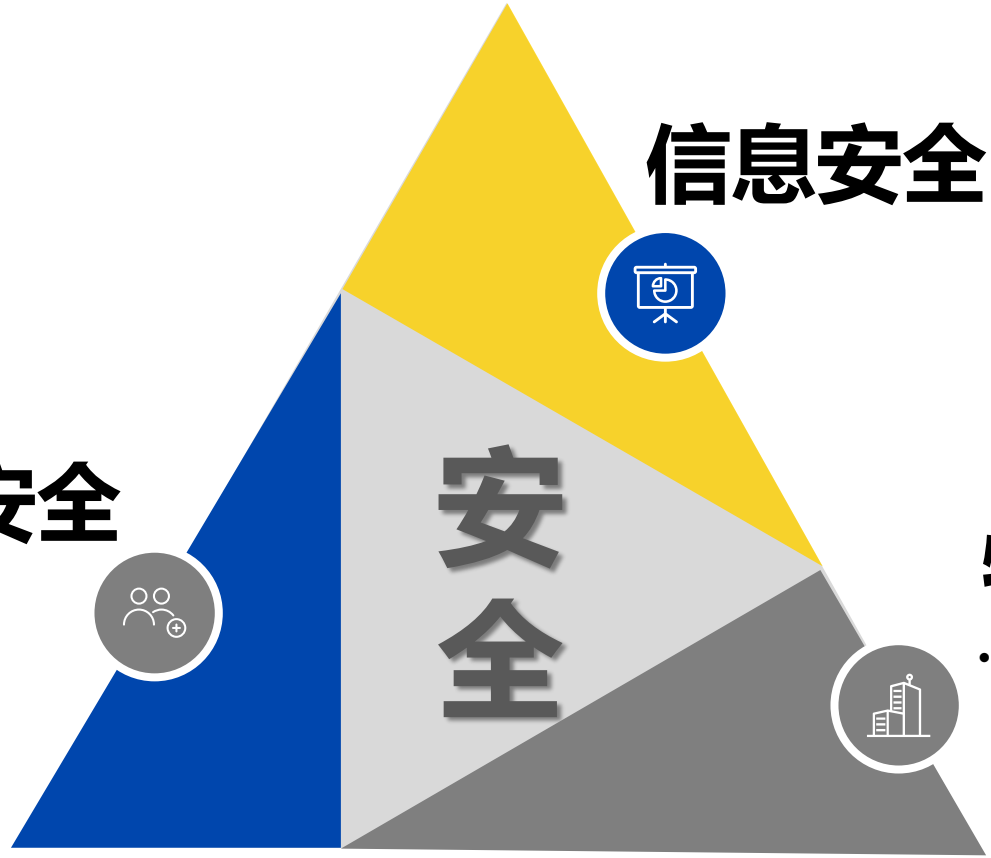
工业控制系统

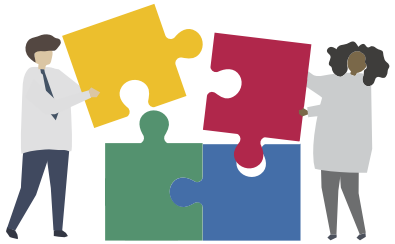
- 变电站自动化
- 工厂自动化
- 轨道交通
- 过程控制
- 航空航天

工业控制系统与IT信息系统



安全的分类



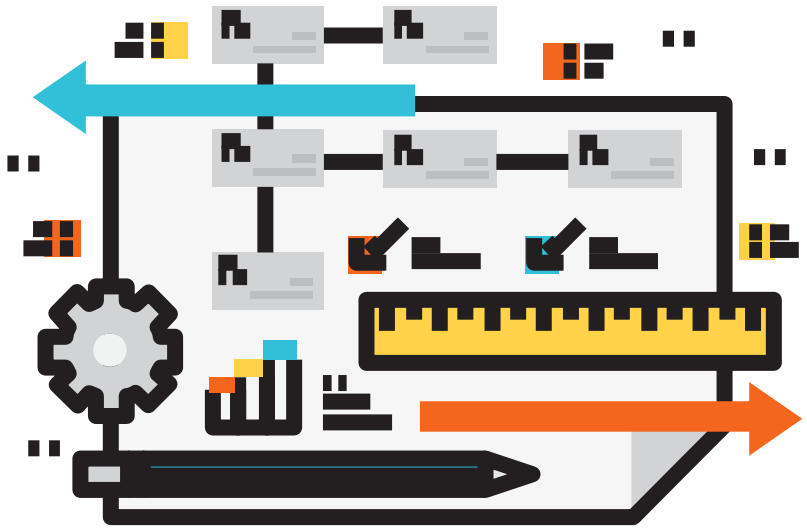


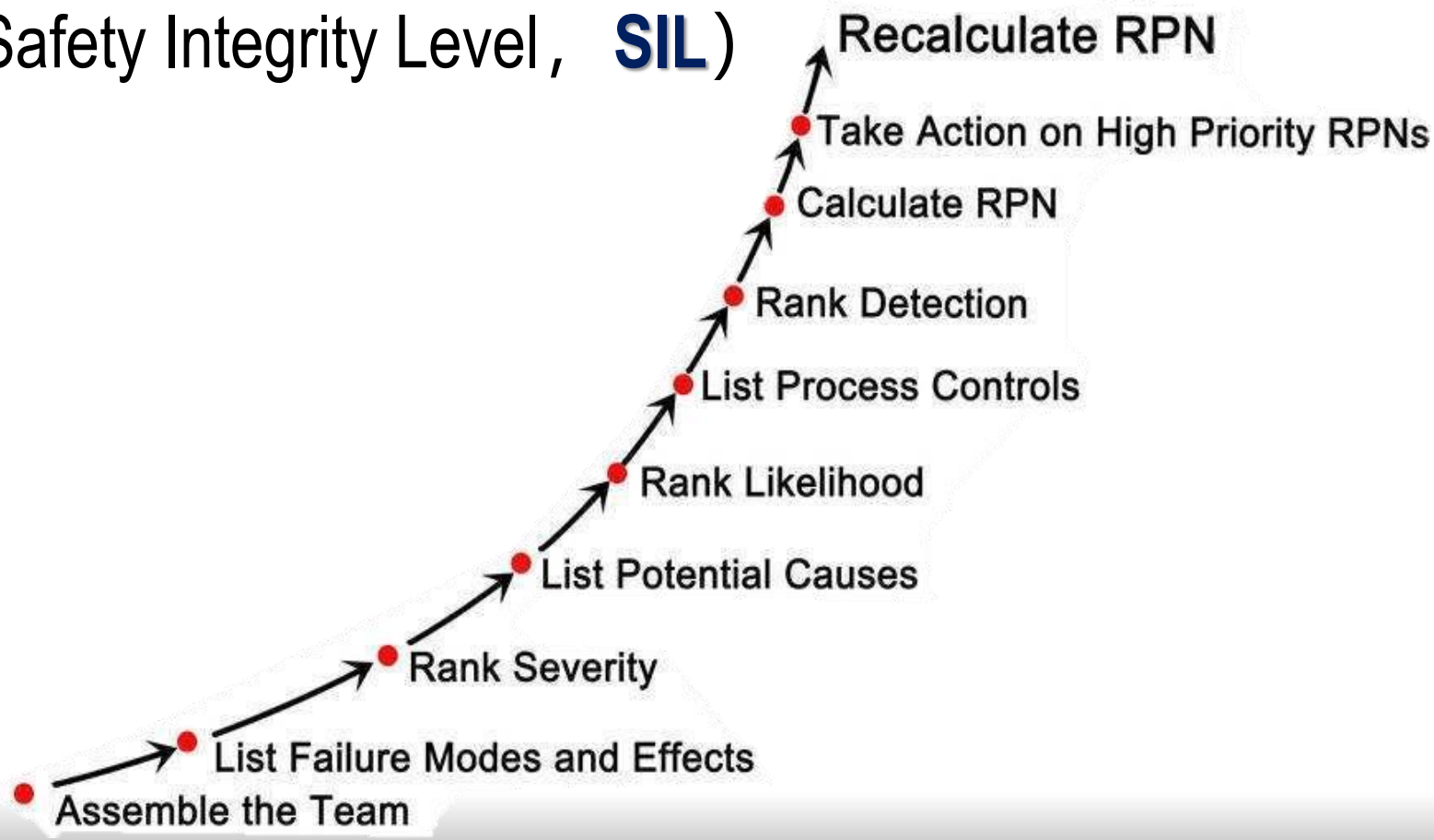
- 减少由于电击、着火、辐射、机械危险、化学危险等因素造成的危害。

功能安全

定义：避免由系统功能性故障导致的不可接受的风险。

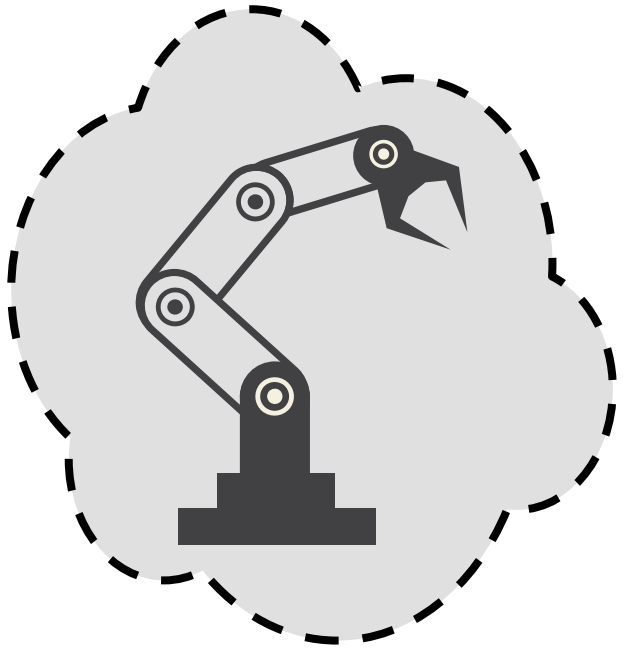
评估：安全完整性等级（Safety Integrity Level，**SIL**）

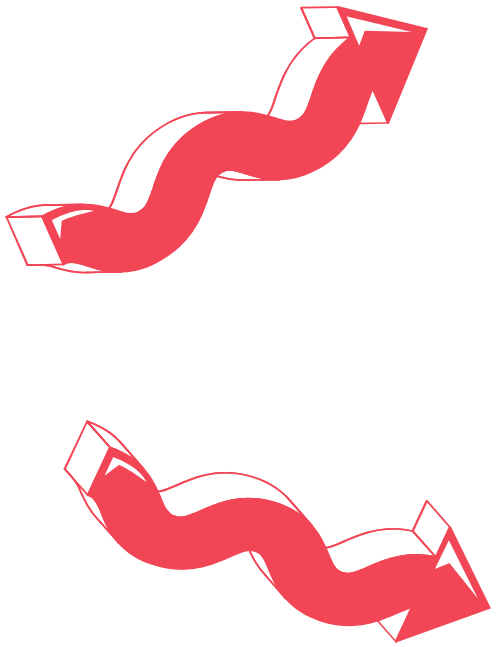


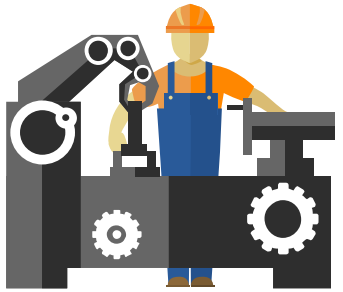


工业功能安全

系统



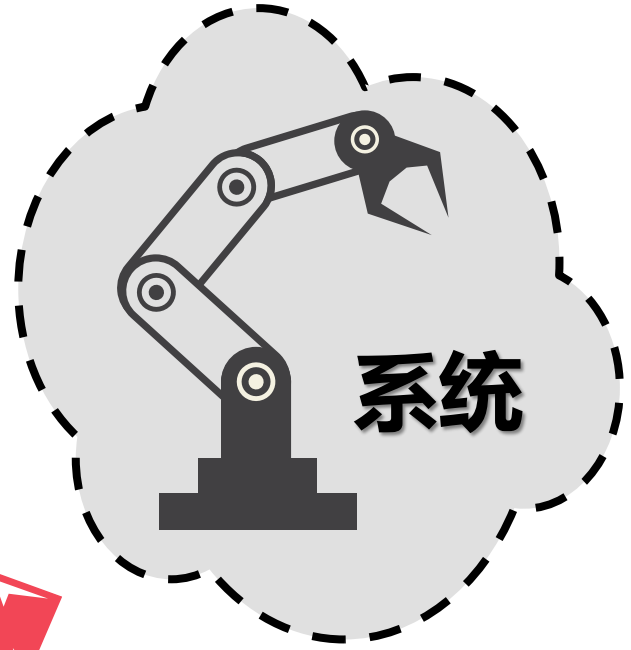




环境

工业信息安全

环境



系统

工业信息安全

① 建立和维护对系统的保护状态；

② 系统资源免于非授权的访问、变更、破坏、损失；

③ 基于计算机系统的能力，防止非授权人员/系统修改软件及其数据和访问系统功能，同时保证授权人员/系统不被阻止；

④ 防止对工业控制系统的非法或有害入侵，或者干扰其正确和计划的操作。

IEC 62443

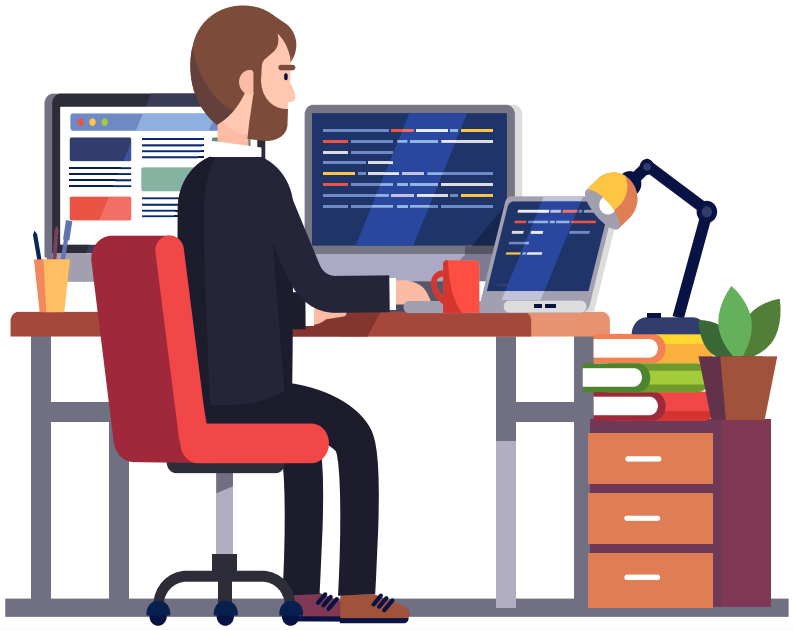
几个误区

- **信息安全技术 ≠ 产品的信息安全**

几个误区

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



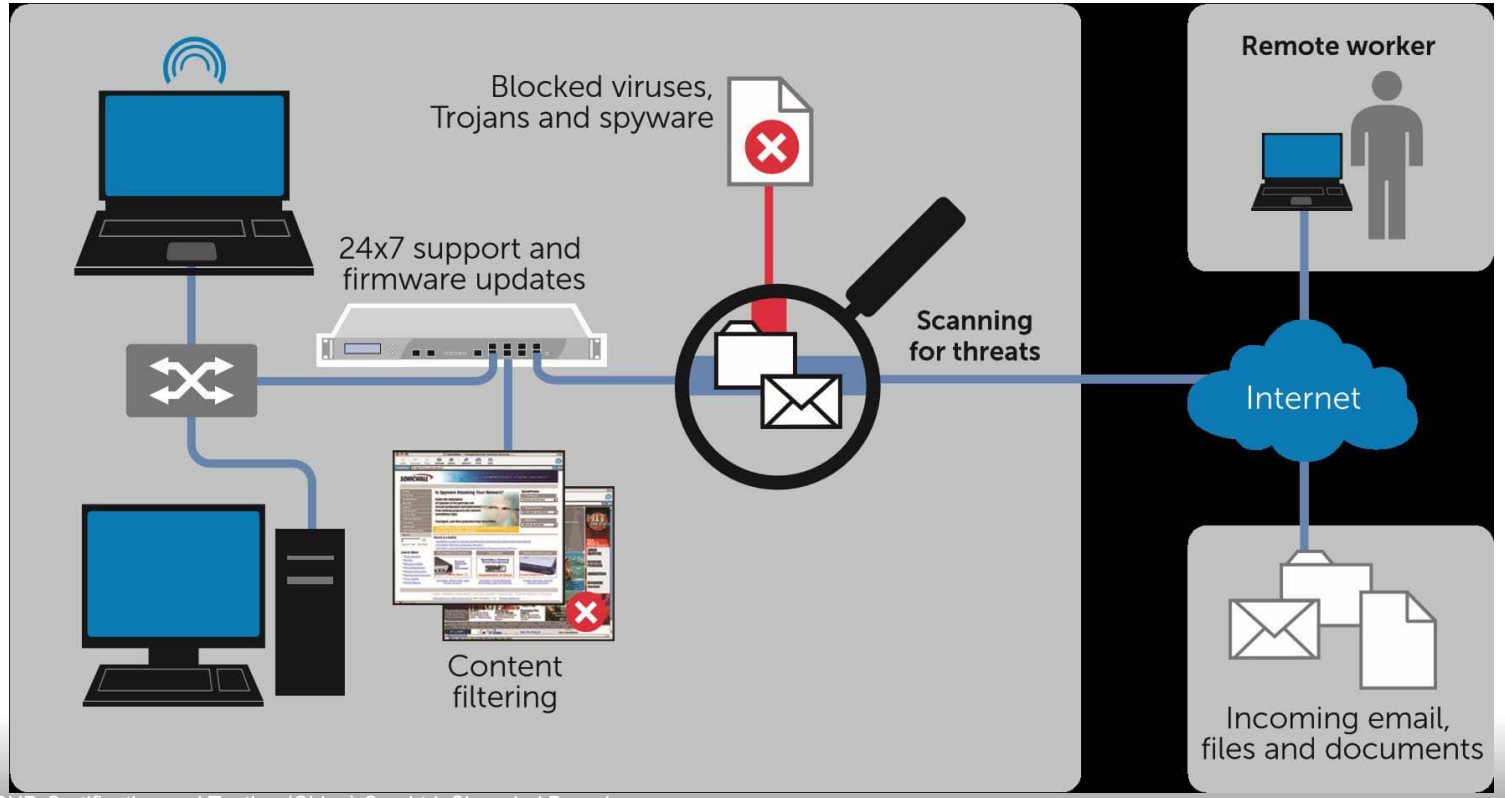
IEC 62443-2-3 Patch Management

IEC 62443-4-1 Update Management

几个误区

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。



几个误区

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….

乌克兰军队被曝使用默认账号密码“admin”和“123456”

2018-09-28 17:30　　国防部 / 俄罗斯

在网络上，账号密码基本上是最流行也是最广泛的保密手段，无论是上QQ，挂VPN，登录局域网，都有机会用到一个账号与密码。一般而言，有些账户系统会直接提供一个默认账户密码以供用户直接使用，比如路由器就是如此，它的默认账号密码就贴在它的机器上，而且很多人都不会更改这个账号密码。

不过如果一个国家军队的安全系统也用的默认账号密码会怎么样呢？

还真有这种事儿，近日，乌克兰记者亚历山大·杜宾斯基就发现乌克兰军队的“第聂伯罗”自动化控制系统的用户名和密码分别是“admin”和“123456”。

几个误区

网易首页 > 数码频道 > 正文

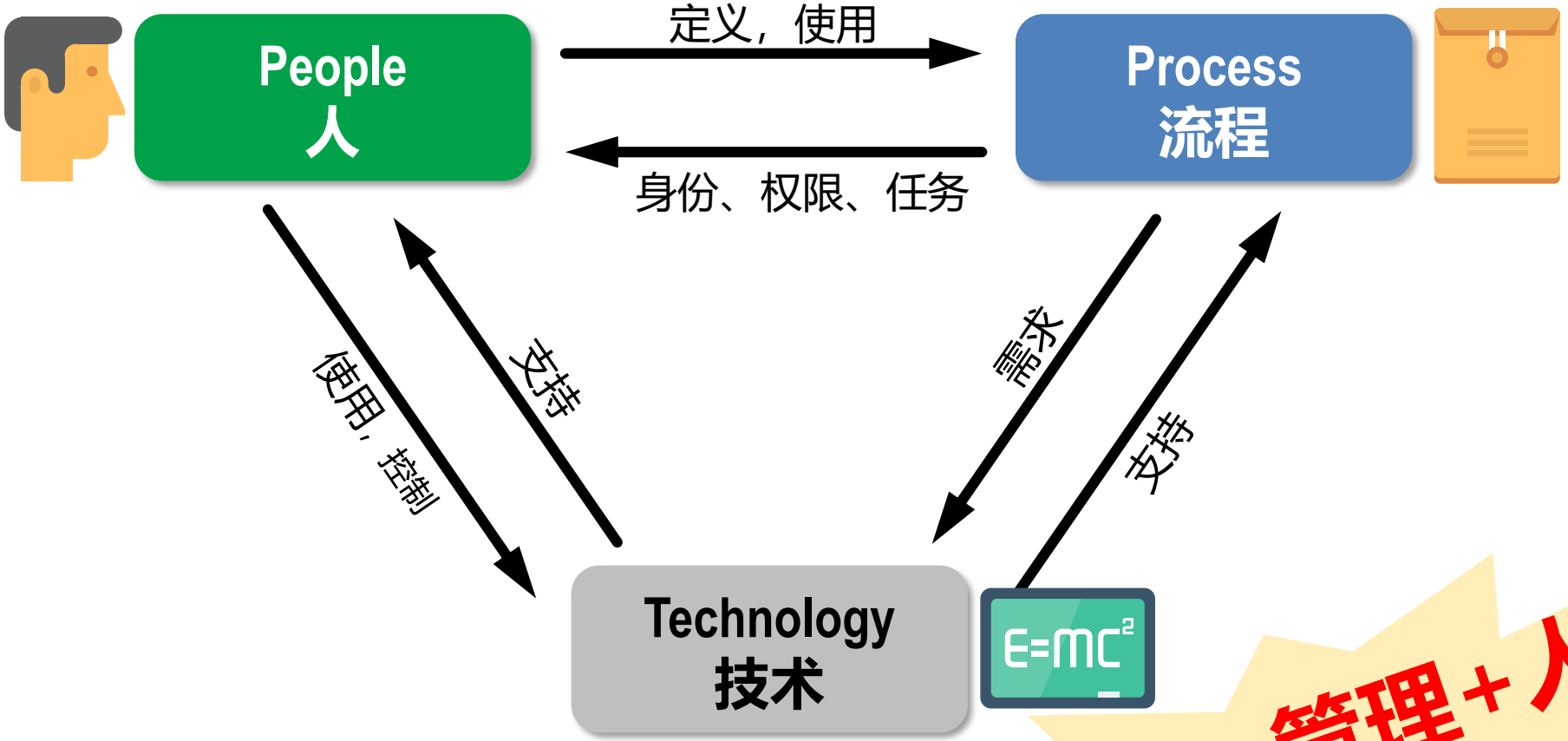
BBC纪录片曝光了铁路控制中心的密码“Password3”

2015-05-05 11:34:06 来源: cnbeta网站(台州) 举报

分享到：

摘要：BBC2台上周播出了纪录片《Nick and Margaret: The Trouble with Our Trains》，展现了私有化20多年后英国铁路网络的悲惨现状。但在两位主持人参观伦敦滑铁卢车站Wessex Integrated控制中心时，摄像机拍下了控制中心的密码（如图所示）。画面中的密码非常清晰，也非常引人瞩目——

保障信息安全的三大基本手段



技术＋管理＋人

目录

Why is IEC 62443

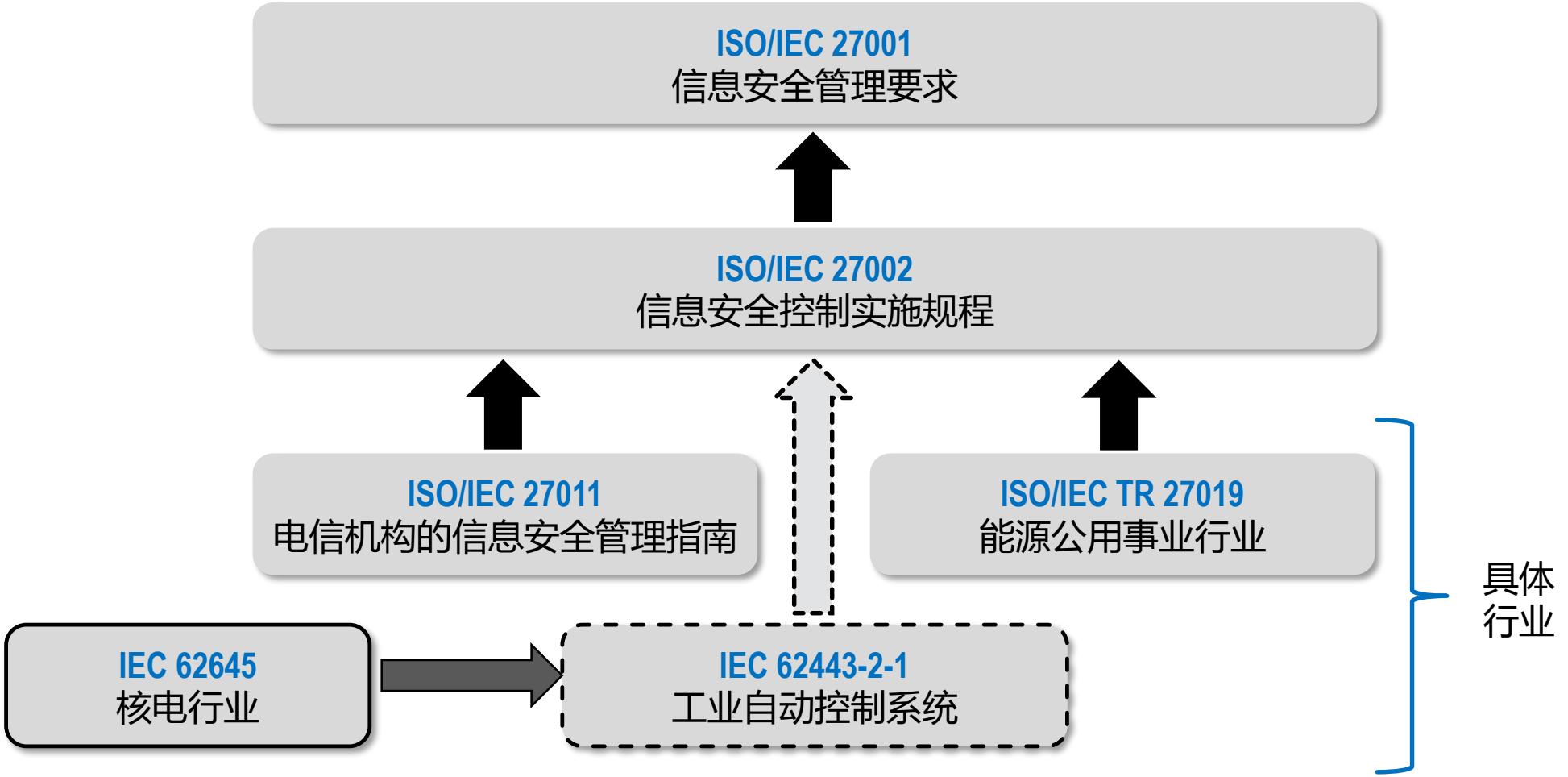
What is IEC 62443

Why is IEC 62443?

ISO 27001

等级保护

ISO 27001


ISO/IEC 27001
信息安全管理要求
ISO/IEC 27002
信息安全控制实施规程
ISO/IEC 27011
电信机构的信息安全管理指南
ISO/IEC TR 27019
能源公用事业行业
IEC 62645
核电行业
IEC 62443-2-1
工业自动控制系统
具体
行业

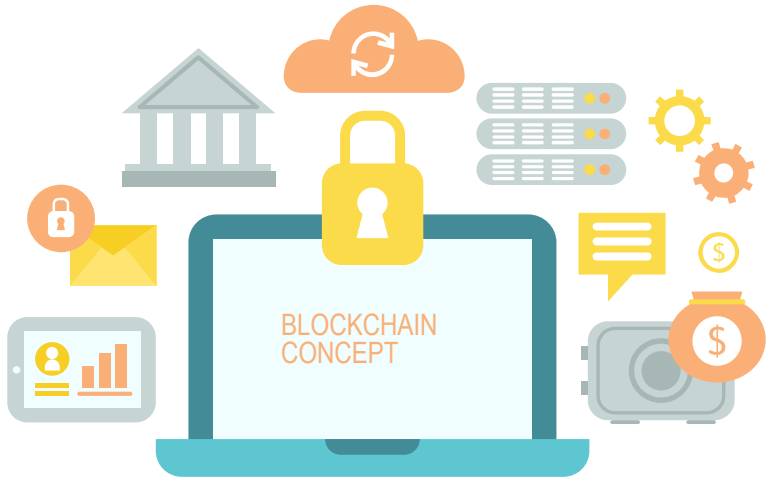
等保相关

2018：等保2.0

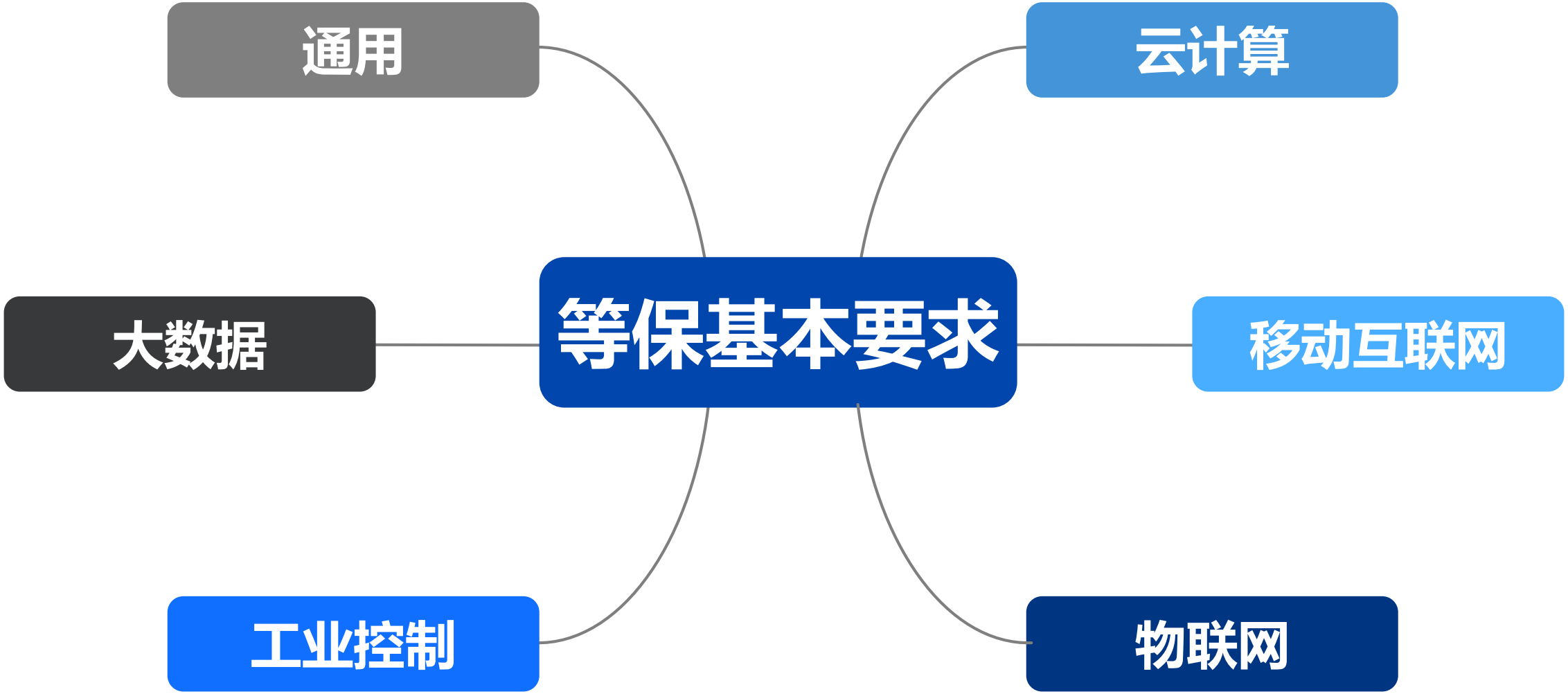
《信息安全技术 网络安全等级保护基本要求》

《网络安全等级保护条例（征求意见稿）》

【适用范围】在中华人民共和国境内**建设、运营、维护、使用网络**，开展网络安全等级保护工作以及监督管理，适用本条例。个人及家庭自建自用的网络除外。



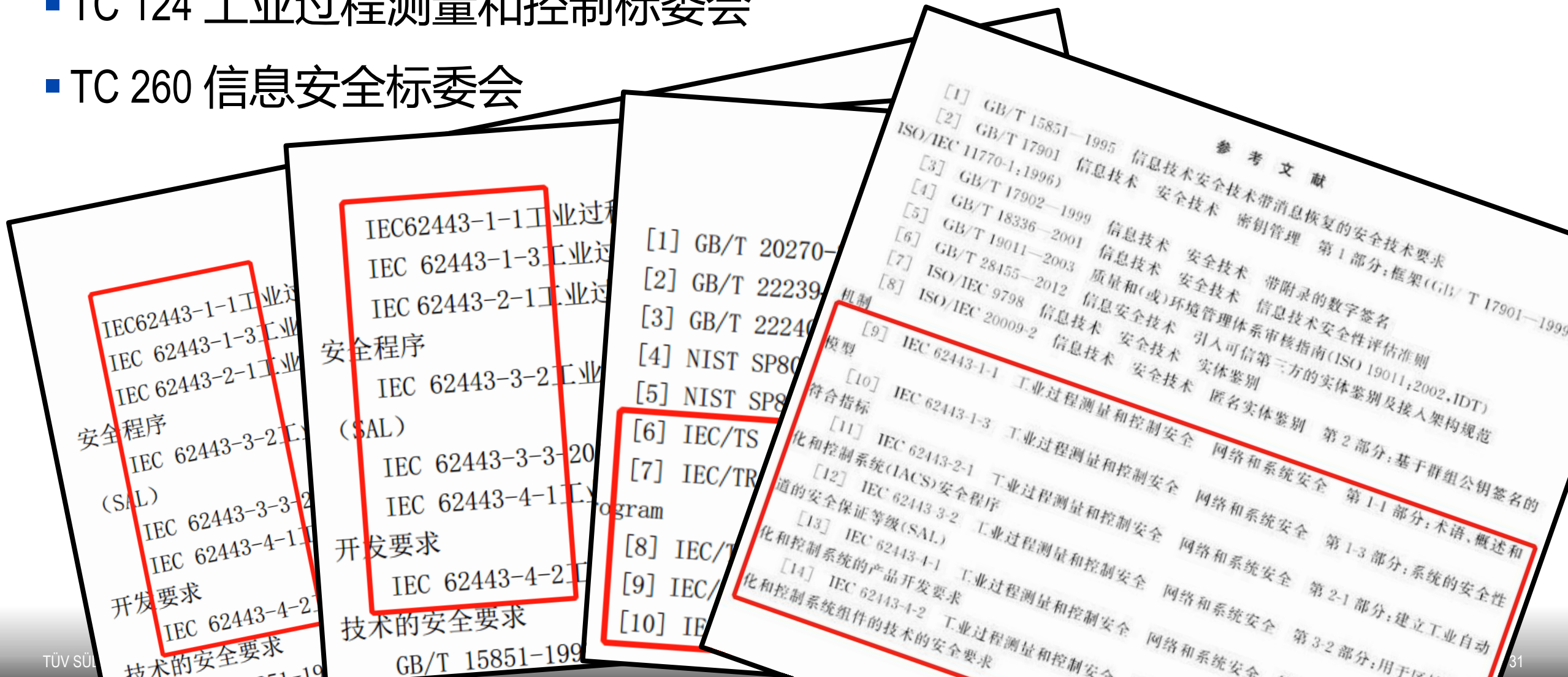
等保相关



国际工业信息安全相关标准组织

国内工业控制系统信息安全标准

- TC 124 工业过程测量和控制标委会
- TC 260 信息安全标委会



What is IEC 62443

Industrial communication networks – Network and system security

工业通信网络——网络和系统安全

IEC 62443 概览

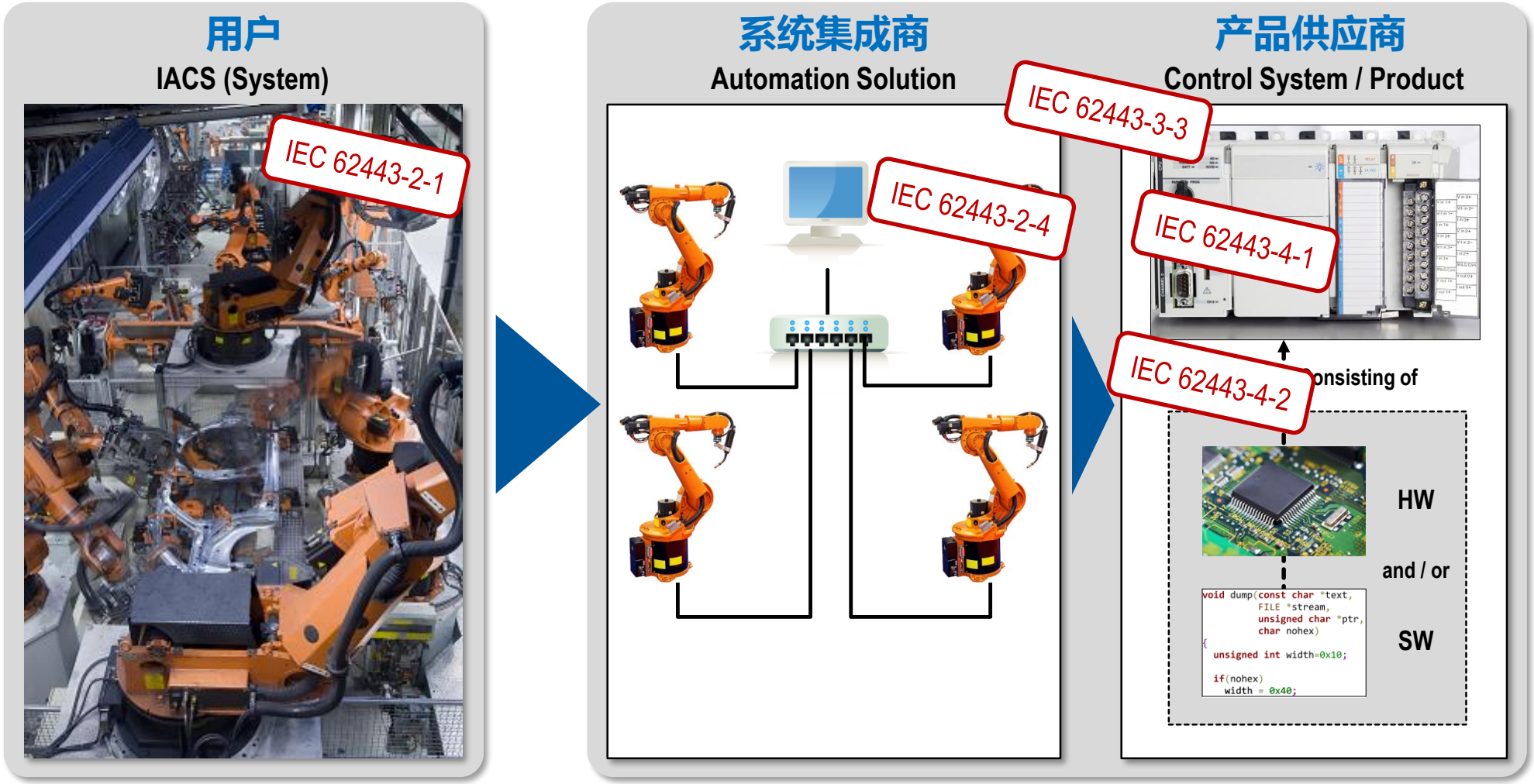
IEC 62443
Industrial communication networks – Network and system security

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		

已发布

IEC 草案通过

IEC 62443 适用范围示例：生产线



目录

IEC 62443: 安全产品

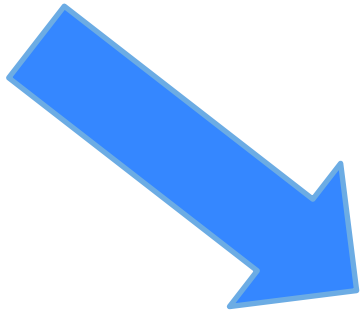
信息安全的产品应该怎么做?

IEC62443的要求——产品和系统

Process
流程

People
人

Technology
技术



产品&系统

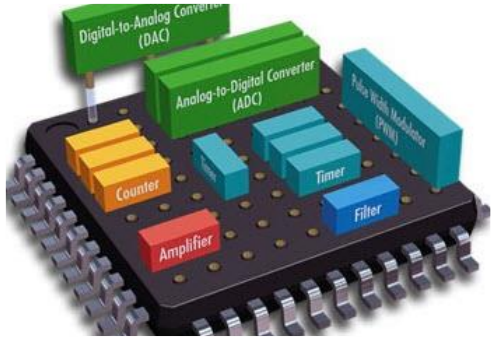
IEC 62443 工业信息安全的7个(维度的)基本要求

- **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)

IEC 62443对产品的要求

IEC 62443-4-2除了对工控产品提出要求，还对部件提出了要求：

软件应用



嵌入式设备

主机设备

网络设备

安全级别 – 是一个向量!

- **Security Level= { IAC, UC, SI, DC, RDF, TRE, RA }**

$$\text{Security Level} = \begin{bmatrix} IAC \\ UC \\ SI \\ DC \\ RDF \\ TRE \\ RA \end{bmatrix}$$

工业信息安全

- 影响信息安全的因数非常复杂，很难用一个简单的数字描述出来。

- **IEC 62443中引入了信息安全等级（Security Level，SL）**
  - 尝试用一种**定量**的方法来处理**一个区域**的信息安全。

Security Level

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:

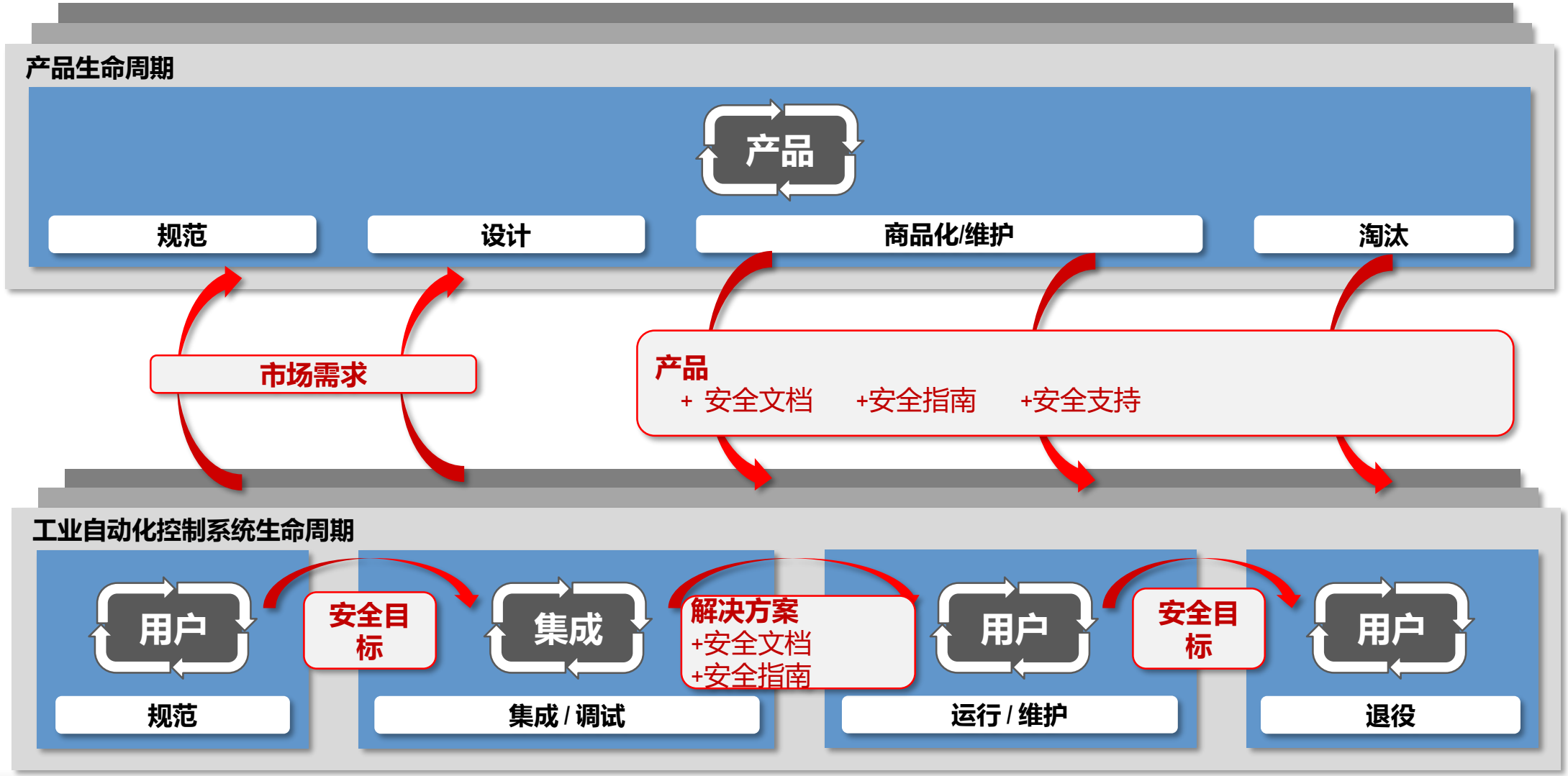
SL	攻击手段	资源	技术	动机
1	偶然的或巧合的			
2	简单	低	通用的	低
3	复杂	中等	特定系统专有	中等
4	复杂	大规模	特定系统专有	强烈

IEC 62443 系统要求 与 安全级别的映射(示例)

	SL1	SL2	SL3	SL4
FR 1 –标识和认证控制(IAC)				
SR 1.1 –用户（人）的标识和认证			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)唯一标识和认证			X	X
The control system shall provide the capability to uniquely identify and authenticate all human users.				
RE (2)非可信网络的多因子认证			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)所有网络的多因子认证				X
The control system shall provide the capability to employ multifactor authentication for all human user access to the control system.				

IEC62443的要求——生命周期

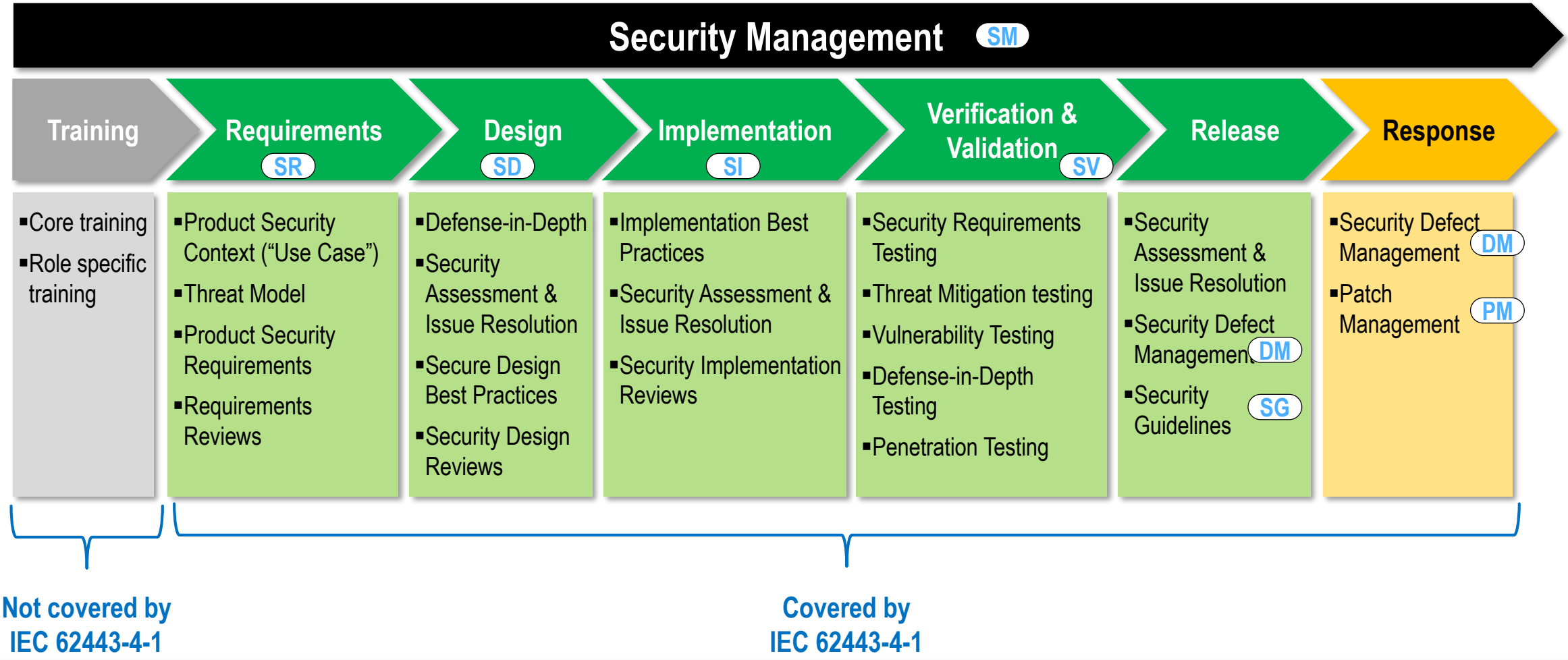
IEC 62443: 安全生命周期



IEC 62443: 安全生命周期之开发商

开发商应该怎么做?

信息安全的生命周期要求 (针对开发)



IEC 62443-4-1: 安全的产品开发流程 (SPDLC)

1.安全管理 (SM)

2.安全需求规范 (SR)

3.安全设计 (SD)

4.安全实现 (SI)

5.安全验证 (SV)

6.缺陷管理 (DM)

7.补丁管理 (PM)

8.安全导则 (SG)

产品如何开发？

开发怎样的产品？

产品是否按设计要求开发？

如何识别处理信息相关事件？

如何提供修补补丁？

如何集成、配置、维护？

IEC 62443: 安全生命周期之集成商

集成商应该怎么做?

IEC 62443-2-4定义了12个功能类别

人员配置	安全保障	设计架构	无线
安全仪表	配置管理	远程登录	事件管理
账户管理	恶意软件	补丁管理	备份恢复

如何评估流程

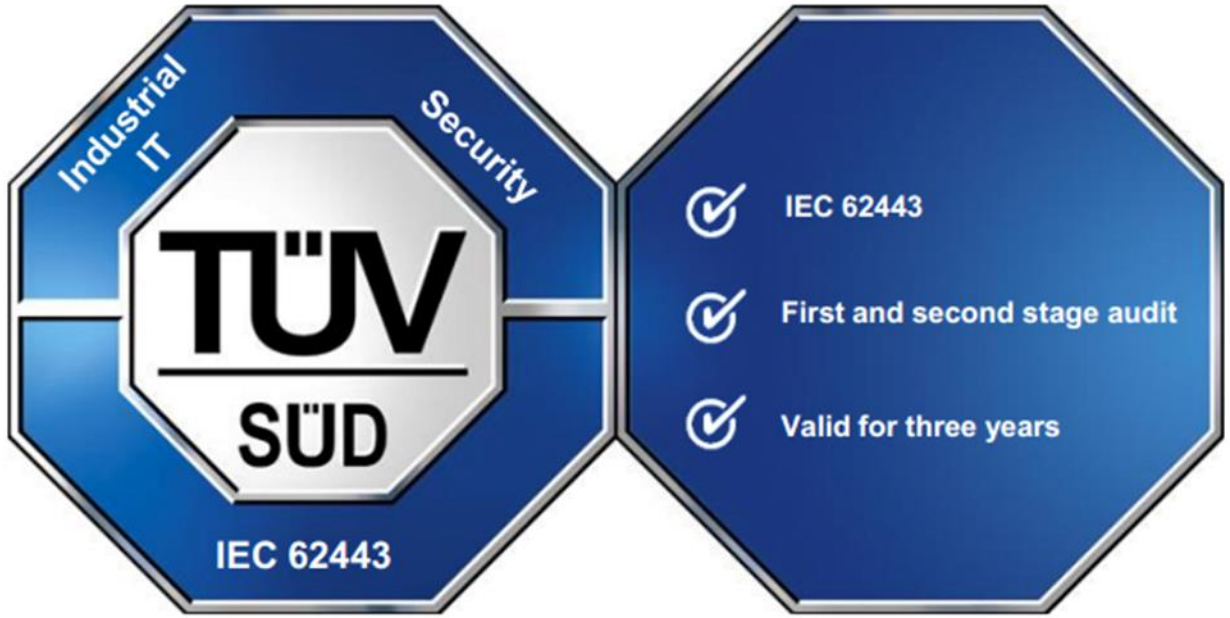
- **Maturity Level 成熟度**
- *“衡量系统集成商在系统集成，维护等活动中满足安全需求的能力”*

IEC 62443定义的4个系统开发商、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

目录

TÜV SÜD工业信息安全认证标识样例



项目案例: 西门子全球首批TÜV 南德IEC 62443认证

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 Dirmeier)

Page 1 of 1

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

证书持有者

- 西门子 (产品生产商)

认证对象

工业自动化产品:

- SIMATIC PCS 7

参考标准

- IEC 62443-4-1
- IEC 62443-3-3

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. 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

证书持有者

- 西门子 (作为设备厂家) 全球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 Life Cycle

参考标准

- IEC 62443-4-1

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 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®

A1 / 04.11

证书持有者

- 西门子 (系统集成商)

认证对象

安全变电站自动化系统，包括变电站自动化设备:
SICAM PAS/PQS, AK3

- HMI: SICAM SCC
- Protection Relay: SIPROTEC 5
- Router/Firewall: RUGGEDCOM
- Switch: RUGGEDCOM

参考标准

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

感谢聆听

陈荻川
Dichuan.Chen@tuv-sud.cn

Mehr Wert.
Mehr Vertrauen.

Add value.
Inspire trust.