欧盟网络弹性法案 (CRA)

开启具有数字元素商品 (PDE) 的全生命周期强制监管时代

CYBER RESILIENCE ACT • (EU) 2024/2847

SIEMENS

第一部分：生效时间表与适用范围

全面剖析 CRA 的关键执行期与管辖红线

SIEMENS

CRA 核心落地时间表

2024年12月10日

法案正式生效

CRA 法案在欧盟公报公布并正式生效，进入约 36 个月的供应链过渡缓冲期。

2026年9月11日

漏洞与安全事故报告义务

过渡期第 21 个月。制造商发现被利用漏洞或重大安全事件时，须在 24 小时内强制报告。

2027年12月11日

全面强制执行

过渡期第 36 个月。未获得合规 CE 标志的商品将被禁止进入欧盟，已有商品强制下架。

SIEMENS

适用范围：谁受影响？谁被豁免？

纳入管辖的产品 (PDE)

指所有直接或间接连接至其他设备或网络的软硬件产品（含配套远程数据处理方案）：

- **消费级 IoT：** 智能手机、路由器、网络摄像头、智能家居设备等。
- **工业级设备：** 工业传感器、机器人、交换机、工业控制系统（OT）。
- **核心组件/软件：** 操作系统、独立浏览器、安全芯片、CPU。

明确获得豁免的领域

已受其他专门法案管辖的高风险领域或特殊用途产品不适用本法：

- **高监管行业：** 医疗器械、民用航空设备、机动车辆。
- **国家安全：** 专为国防、军事或国家安全目的开发的产品。
- **非商业模式：** 纯非商业性开源软件、为单一客户定制的内部私有系统。

SIEMENS

产品风险分类与合格评定程序

产品风险类别	典型涵盖范围 (产品示例)	合规认证与评定方式
		制造商自我评估 (Self-assessment)
默认类/非关键产品 占市场约 90%	普通智能家居设备、外置硬盘、绝大多数消费级物联网设备、基础应用软件等。	确认符合基本安全规范后即可加贴 CE 标志。
重要类 Class I 中低度核心设备	身份管理系统、**家用路由器**、网络交换机、智能门锁、安防监控摄像头、浏览器。	引用统一标准（如看齐 **IEC 62443**），或通过欧盟授权的第三方机构评定。
		强制性第三方评估
重要类 Class II 高风险/核心信任链	企业级网络防火墙、硬件安全模块（HSM）、密钥管理系统、安全芯片等。	必须由欧盟认可的公告机构 (Notified Body) 进行全方位审计。

SIEMENS

制造商的四大核心硬性义务

安全设计 (Security by Design) 开发初期必须进行风险评估和威胁建模。禁用通用默认密码，默认配置必须保障安全，最大化减少受攻击面。

漏洞全周期管理 设立非纯 AI 的单一联系点（SPoC）。在产品寿命期内（通常不少于5年）提供免费的安全和系统更新服务。

软件物料清单 (SBOM) 强制建立并维护标准化软件物料清单，实时追溯上游第三方库与开源组件，确保软件供应链透明可控。

自动更新合规规范 消费级设备应默认支持自动安全更新并允许用户退出；而在工业等 OT 环境中，为规避意外停机风险，避免强制自动更新。

SIEMENS

全供应链连带责任与重罚

严格的连带合规审查

CRA 终结了“仅监管研发方”的时代。**进口商**与**分销商**必须严格核验产品技术文档与 CE 标志。若以自身商标进行贴牌销售，将被等同于制造商，承担全部法律责任。

⚠ 巨额违规代价

如果不履行合规义务或蓄意提供虚假数据，企业将面临极具威慑力的欧盟制裁：

最高 1500万欧元 **或全球年营业额** 2.5%

* 以较高者为准，同时不合规产品将被强制召回或限期销售下架。

SIEMENS

IEC 62443 标准介绍

工业自动化和控制系统 (IACS) 架构下的全球网络安全基准

核心价值与定义

什么是 IEC 62443，它为何在 OT 领域不可或缺？

IT 与 OT 的优先级对立

传统的 IT 安全聚焦于数据保护，而工业运营 (OT) 的安全核心在于物理安全与业务连续性。

IT 安全 (CIA)

保密性 > 完整性 > 可用性

OT 安全 (AIC)

可用性 > 完整性 > 保密性 (安全性 Safety 为前提)

标准的四层架构体系

通用层 (General)

1-x 系列：术语、概念、模型及度量指标。

政策与流程

2-x 系列：安全管理体系、修补管理及供应商要求。

系统层 (System)

3-x 系列：技术安全要求、区域与导轨建模。

组件层 (Component)

4-x 系列：产品开发生命周期及组件级安全要求。

安全等级(SL 1 - SL 4)

SL 4

应对有组织的高级威胁

- **SL 1:** 防止无意或偶然的违规。
- **SL 2:** 防止使用简单工具的低动机攻击。
- **SL 3:** 防止使用专业技能的中等资源攻击。
- **SL 4:** 防止利用国家级资源的精锐攻击。

七大基础安全要求 (FR)

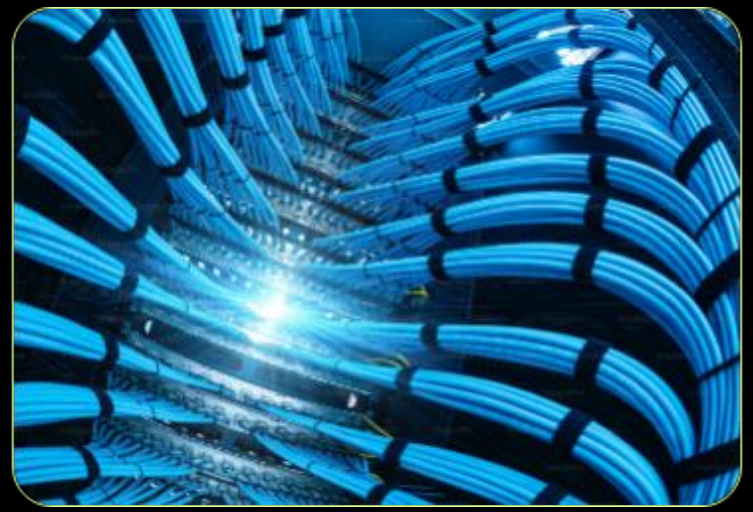
- 身份识别与认证控制 (FR1)
- 使用控制 (FR2)
- 系统完整性 (FR3)
- 数据机密性 (FR4)
- 受限数据流 (FR5)
- 及时响应事件 (FR6)
- 资源可用性 (FR7)

* 每项要求根据 SL 等级有不同的实施深度

产业链中的核心角色

资产拥有者

定义安全政策、执行风险评估并运行安全管理体系。



产品供应商

在产品开发生命周期中嵌入安全能力 (SL-C)。

系统集成商

将组件整合为安全系统，满足特定的 SL-T 目标。

网络安全全生命周期

1. 风险评估

识别 SuC，执行高层与详细风险分析。

2. 设计与实施

制定 CSRS，应用补偿性安全措施。

3. 验证与集成

通过测试验证是否达到预期的安全等级。

4. 运维与管理

持续监控、事件管理与定期审计。

SL 标志：目标、能力与达成

标志类型	定义 (Definition)	责任方 (Responsibility)
SL-T (Target)	目标安全等级：基于风险评估确定的期望状态。	资产拥有者 (Asset Owner)
SL-C (Capability)	能力安全等级：系统或产品原生支持的安全防御限度。	产品供应商 (Supplier)
SL-A (Achieved)	达成安全等级：系统在实际运行时验证到的安全表现。	系统集成商 / 资产拥有者

SICAM A8000
变电站安全数据网关解决方案

SIEMENS

电力系统
供应链安全中的网络安全

§ 德国：《信息技术安全法》；
欧洲：《欧洲网络信息安全指令》

ISO/IEC 27001
ISO/IEC 27002

操作员 — IT基础设施（办公IT）

ISO/IEC 27001
ISO/IEC 27019

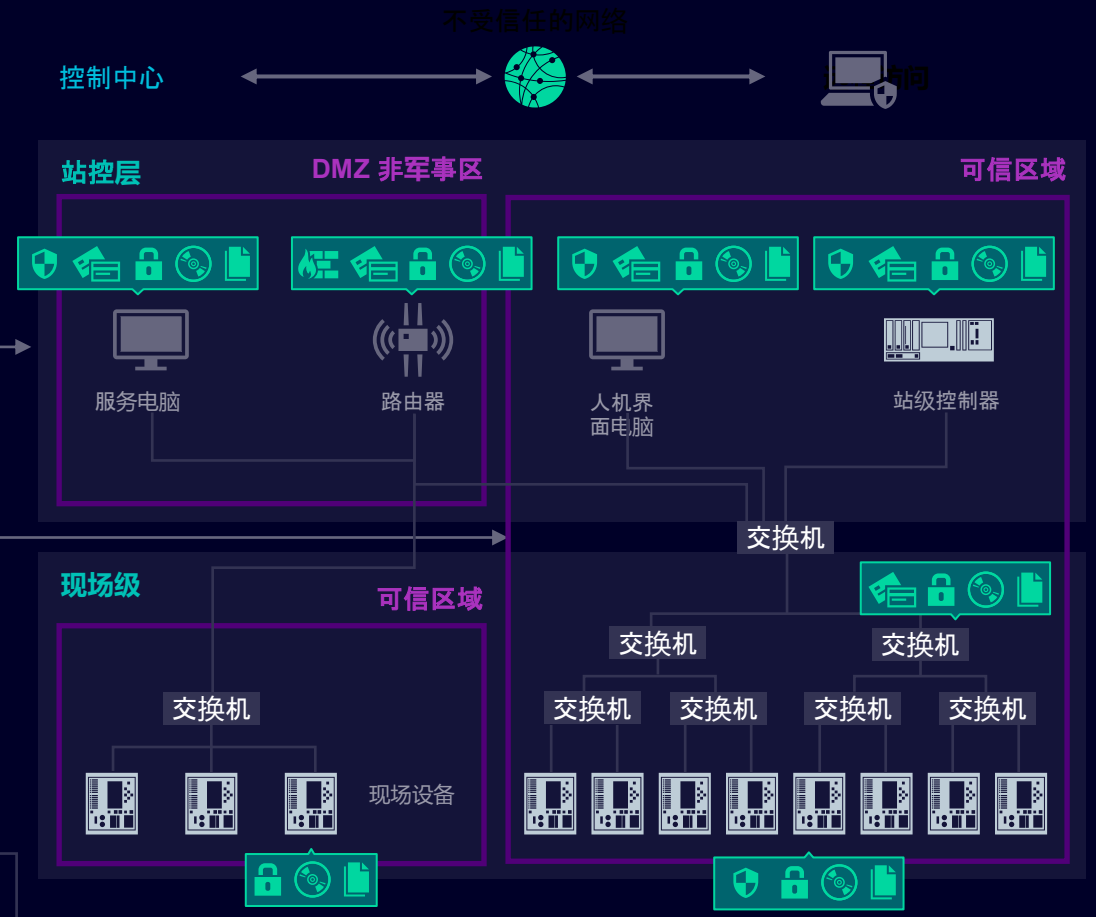
要求

集成商 — IT基础设施（办公IT）

IEC 62443-2-4
IEC 62443-3-3
IEC 62351

产品供应商 — IT基础设施（办公IT）

IEC 62443-4-1
IEC 62443-4-2
IEC 62351



程序性流程，例如运营商的信息安全管理体系 (ISMS)、集成商和产品供应商的开发流程
功能性方面，例如安全级别、安全措施强度
技术方面，例如基于角色的访问控制（RBAC）、安全通信协议……

SIEMENS

SICAM A8000网络安全

防火墙

通过集成软件防火墙实现 TCP/IP 网络隔离

固件签名

防止 固件 操纵

安全日志

断电后仍能存储 SYSLOG 事件

TLS加密

符合 IEC 62351-3 标准的基于证书的加密，适用于 IEC 协议

VLAN 支持

VLAN支持 符合 IEEE 802.1Q 标准

网络认证

基于证书的网络认证符合 IEEE 802.1x 标准

通过EST进行X.509证书交换

自动的 证书 通过 EST与 SICAM GridPass

基于角色的访问控制

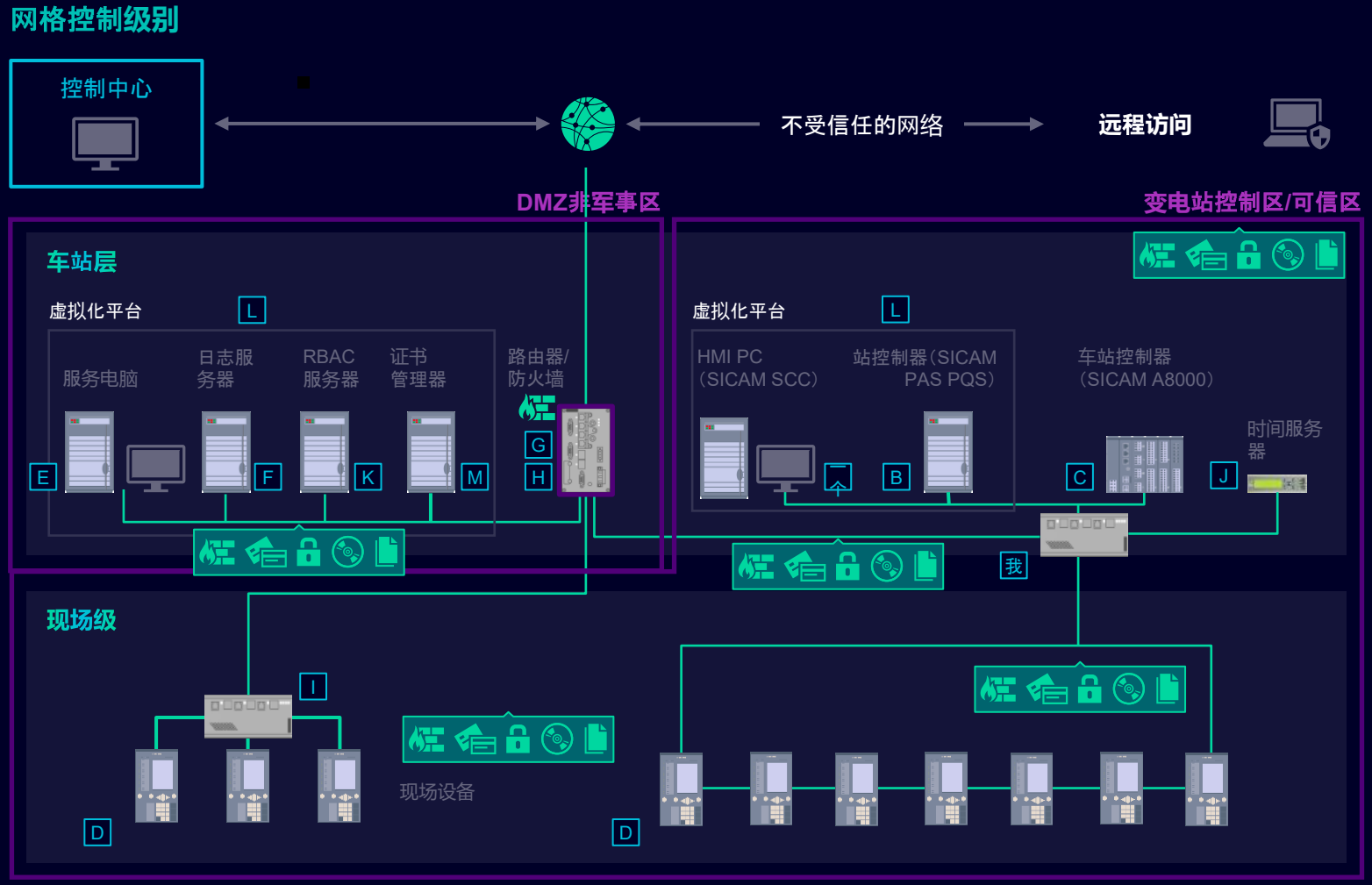
根据 IEC 62351-8 标准，基于角色的访问控制 (RBAC) 确保每个用户只能行使与其分配角色相对应的权限。

可配置系统功能

每个通信接口可选择性地启用单个或多个系统功能

SIEMENS

电力系统网络安全：
保障能源自动化系统



网络安全措施

- 访问控制和账户管理
- 安全日志记录和监控
- 系统加固
- 安全补丁、备份和恢复
- 恶意软件防护
- 数据保护、数据完整性和系统架构
- 安全远程访问

IEC 62443认证解决方案

经 TÜV SÜD 认证

- IEC 62443-2-4 – 集成商流程
- IEC 62443-3-3 – 技术功能

SIEMENS

SICAM 8
Relevant Standards / Norms related to Cyber Security in our area

IEC 62443
Security for Industrial Automation and Control Systems (IACS)

General	Policies & Procedures	System	Component/Product
1-1 Terminology, concepts and models	2-1 Security program requirements for IACS asset owners	3-1 Security technologies for IACS	4-1 Secure Product Development Lifestyle Requirements ✓
1-2 Master glossary of terms and abbreviations	2-2 Security Program Rating	3-2 Security Risk Assessment and System Design	4-2 Technical security requirements for IACS components ✓
1-3 System security conformance metrics	2-3 Patch management in the IACS environment	3-3 System security requirements and security levels ✓	
1-4 ICAS security lifecycle and use-cases	2-4 Security program requirements for IACS service providers ✓		
1-5 Scheme for IEC 62443 Cybersecurity Profiles	2-5 Implementation guidance for ICAS asset owners		

Operator — Product Supplier

System Integrator

Process requirements — Technical requirements

IEC 62443 addresses organizational and technical requirements for

- Operator
- Integrator
- Product Vendor

Enables design of security solutions for different purposes through security measures of varying strength.

Enables **certification of solutions and processes**.

✓ certificate available in SI EA

✓ certificate available for SICAM A8000

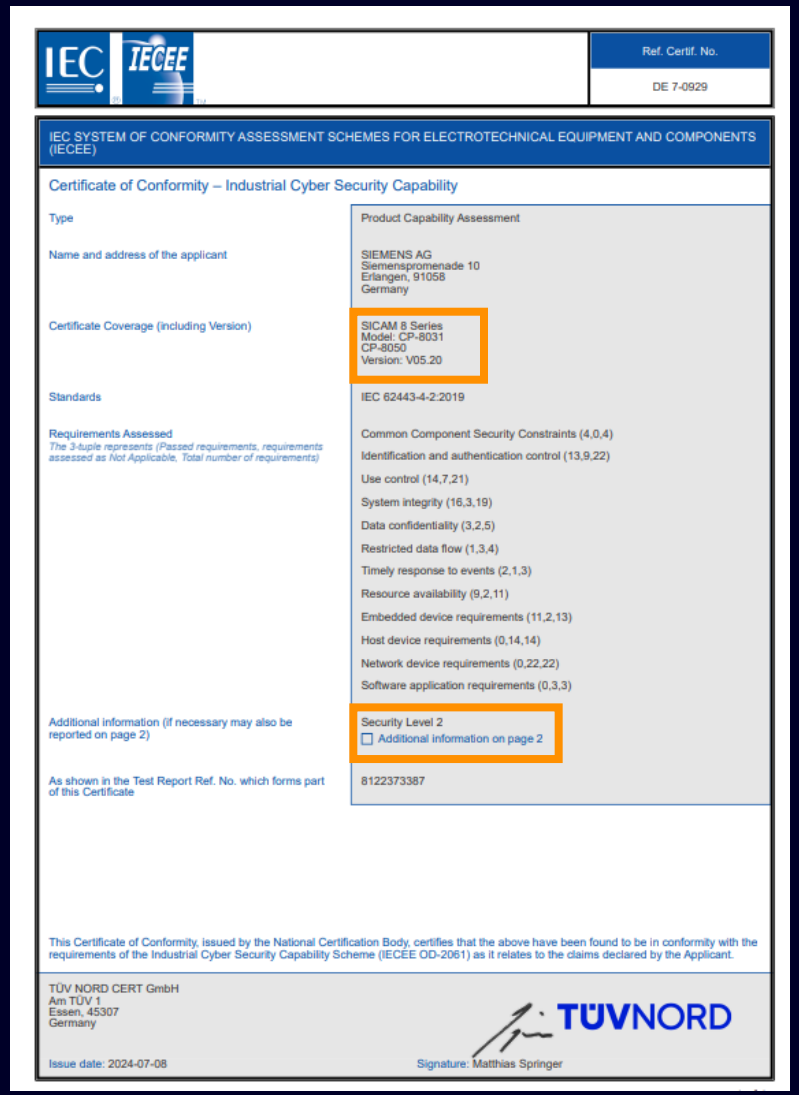
SIEMENS

Certification by TÜV Nord of SICAM A8000 CP-8050/31 acc. IEC 62443-4-2

SICAM A8000 is Front Runner

IEC 62443-4-2 certification with SL-2 for SICAM A8000

CP-8050 / CP-8031



IEC IECEE

Ref. Certif. No.
DE 7-0929

IEC SYSTEM OF CONFORMITY ASSESSMENT SCHEMES FOR ELECTROTECHNICAL EQUIPMENT AND COMPONENTS (IECEE)

Certificate of Conformity – Industrial Cyber Security Capability

Type	Product Capability Assessment
Name and address of the applicant	SIEMENS AG Siemenspromenade 10 Erlangen, 91058 Germany
Certificate Coverage (including Version)	SICAM 8 Series Model: CP-8031 CP-8050 Version: V05.20
Standards	IEC 62443-4-2:2019
Requirements Assessed *The 3-tuple represents (Passed requirements, requirements assessed as Not Applicable, Total number of requirements)*	Common Component Security Constraints (4,0,4) Identification and authentication control (13,9,22) Use control (14,7,21) System integrity (16,3,19) Data confidentiality (3,2,5) Restricted data flow (1,3,4) Timely response to events (2,1,3) Resource availability (9,2,11) Embedded device requirements (11,2,13) Host device requirements (0,14,14) Network device requirements (0,22,22) Software application requirements (0,3,3)
Additional information (if necessary may also be reported on page 2)	Security Level 2 ☐ Additional information on page 2
As shown in the Test Report Ref. No. which forms part of this Certificate	8122373387

This Certificate of Conformity, issued by the National Certification Body, certifies that the above have been found to be in conformity with the requirements of the Industrial Cyber Security Capability Scheme (IECEE OD-2061) as it relates to the claims declared by the Applicant.

TÜV NORD CERT GmbH
Am TÜV 1
Essen, 45307
Germany

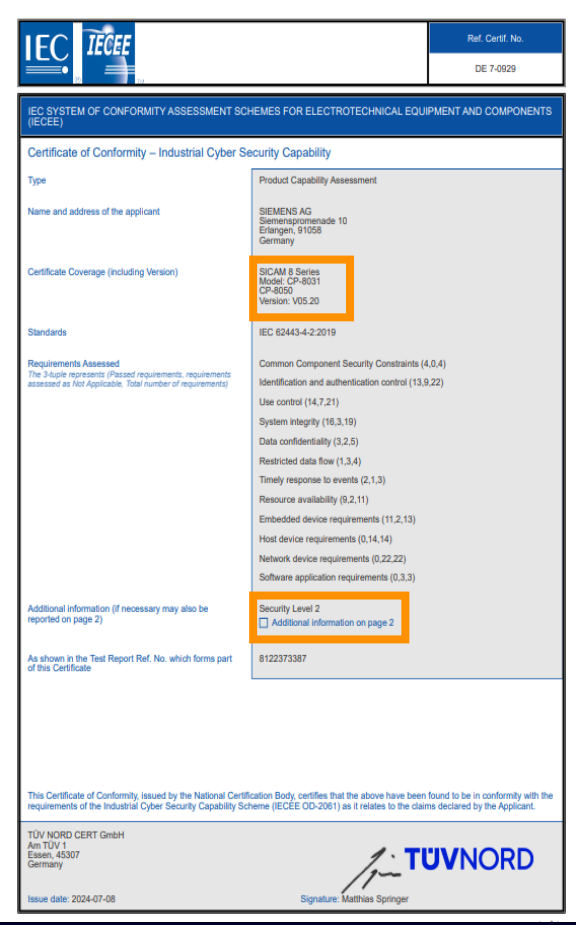
TÜVNORD

Issue date: 2024-07-08

Signature: Matthias Springer

SIEMENS

Cybersecurity in the Power Grid
… calls for a Holistic Approach



IEC IECEE — Ref. Certif. No. DE 7-0929

IEC SYSTEM OF CONFORMITY ASSESSMENT SCHEMES FOR ELECTROTECHNICAL EQUIPMENT AND COMPONENTS (IECEE)

Certificate of Conformity – Industrial Cyber Security Capability

Type	Product Capability Assessment
Name and address of the applicant	SIEMENS AG Siemenspromenade 10 Erlangen, 91058 Germany
Certificate Coverage (including Version)	SICAM 8 Series Model: CP-8031 CP-8050 Version: V05.20
Standards	IEC 62443-4-2:2019
Requirements Assessed *The 3-tuple represents (Passed requirements, requirements assessed as Not Applicable, Total number of requirements)*	Common Component Security Constraints (4,0,4) Identification and authentication control (13,9,22) Use control (14,7,21) System integrity (16,3,19) Data confidentiality (3,2,5) Restricted data flow (1,3,4) Timely response to events (2,1,3) Resource availability (9,2,11) Embedded device requirements (11,2,13) Host device requirements (0,14,14) Network device requirements (0,22,22) Software application requirements (0,3,3)
Additional information (if necessary may also be reported on page 2)	Security Level 2 ☐ Additional information on page 2
As shown in the Test Report Ref. No. which forms part of this Certificate	8122373387

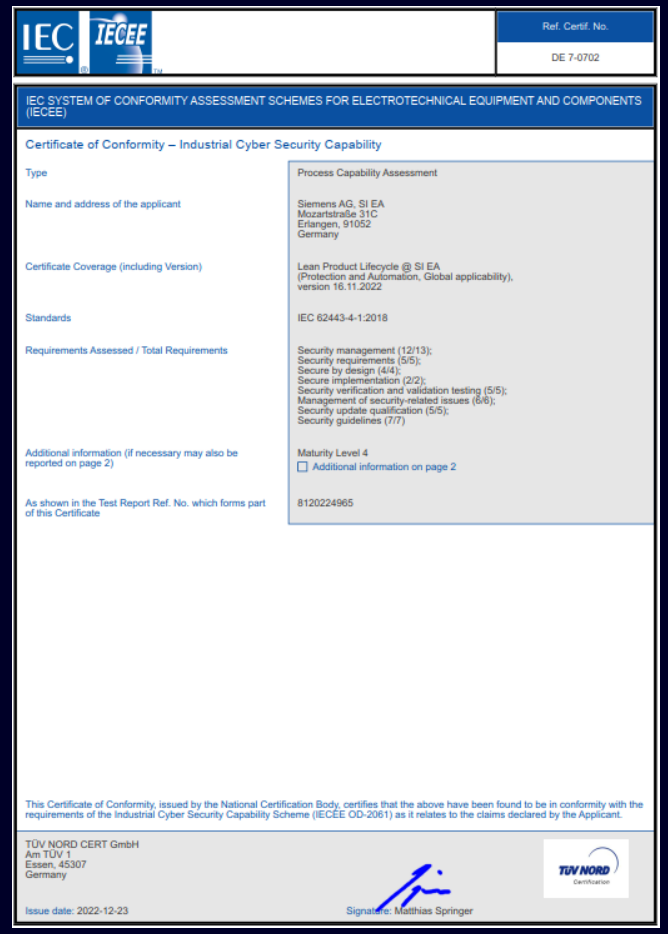
This Certificate of Conformity, issued by the National Certification Body, certifies that the above have been found to be in conformity with the requirements of the Industrial Cyber Security Capability Scheme (IECEE OD-2061) as it relates to the claims declared by the Applicant.

TÜV NORD CERT GmbH
Am TÜV 1
Essen, 45307
Germany

Issue date: 2024-07-08

Signature: Matthias Springer

TÜVNORD



IEC IECEE — Ref. Certif. No. DE 7-0702

IEC SYSTEM OF CONFORMITY ASSESSMENT SCHEMES FOR ELECTROTECHNICAL EQUIPMENT AND COMPONENTS (IECEE)

Certificate of Conformity – Industrial Cyber Security Capability

Type	Process Capability Assessment
Name and address of the applicant	Siemens AG, SI EA Mozartstraße 31C Erlangen, 91052 Germany
Certificate Coverage (including Version)	Lean Product Lifecycle @ SI EA (Protection and Automation, Global applicability), version 16.11.2022
Standards	IEC 62443-4-1:2018
Requirements Assessed / Total Requirements	Security management (12/13); Security requirements (5/5); Secure by design (4/4); Secure implementation (2/2); Security verification and validation testing (5/5); Management of security-related issues (8/8); Security update qualification (5/5); Security guidelines (7/7)
Additional information (if necessary may also be reported on page 2)	Maturity Level 4 ☐ Additional information on page 2
As shown in the Test Report Ref. No. which forms part of this Certificate	8120224965

This Certificate of Conformity, issued by the National Certification Body, certifies that the above have been found to be in conformity with the requirements of the Industrial Cyber Security Capability Scheme (IECEE OD-2061) as it relates to the claims declared by the Applicant.

TÜV NORD CERT GmbH
Am TÜV 1
Essen, 45307
Germany

Issue date: 2022-12-23

Signature: Matthias Springer

TÜV NORD Certification

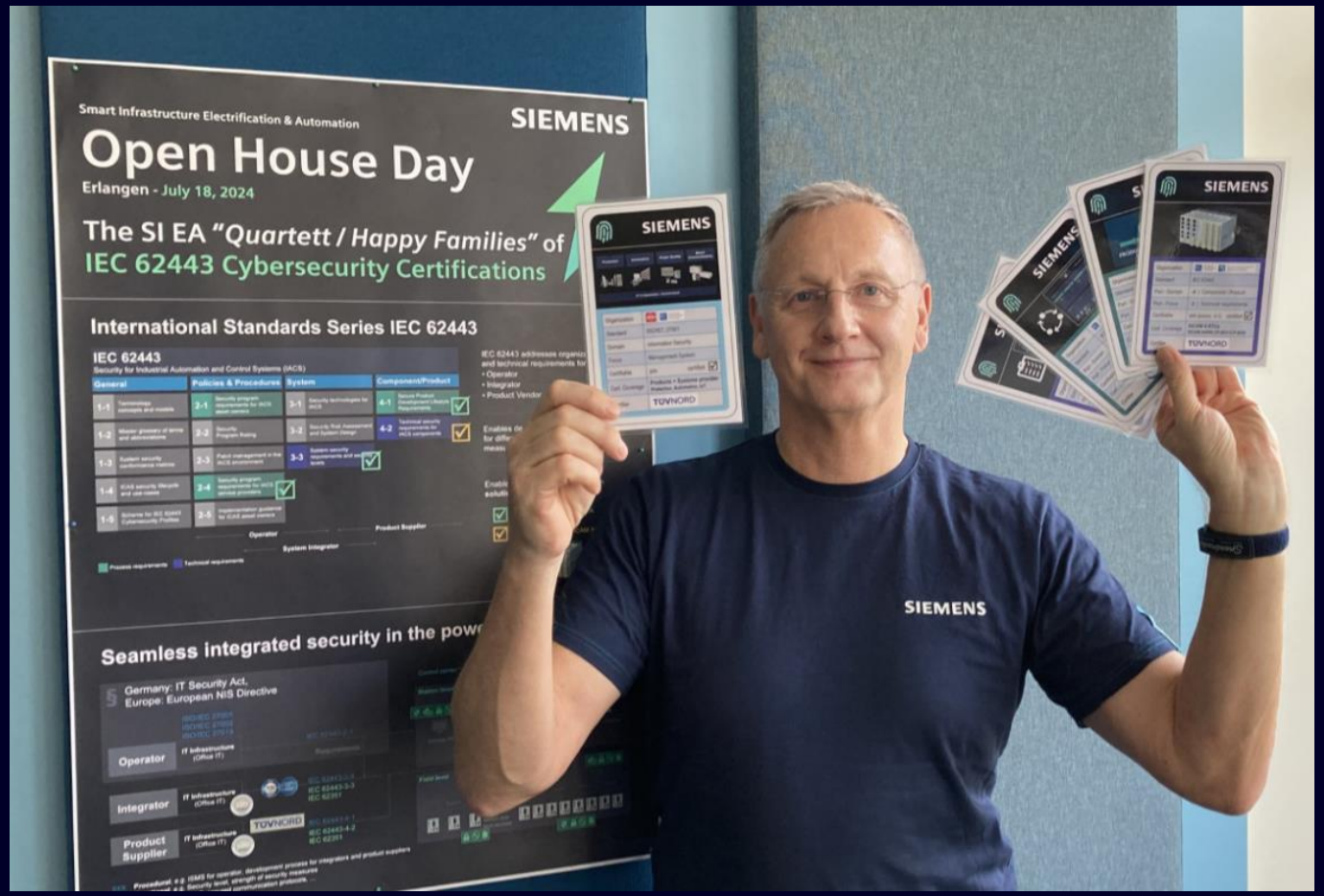
Certificate for our Product Development Lifecycle process acc. IEC 62443-4-1
=> benchmark: we got the highest maturity level 4

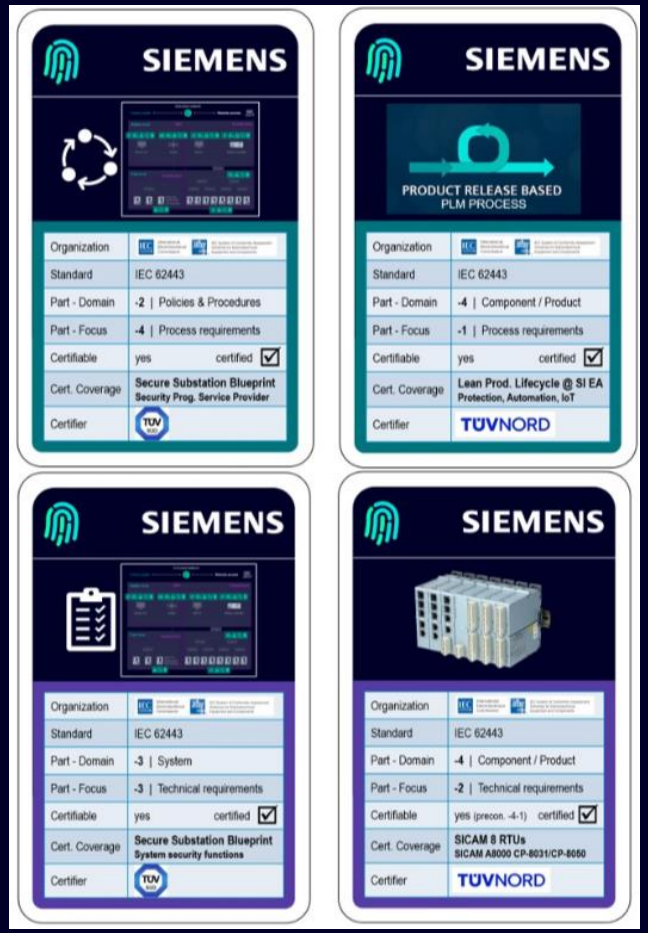
Certificate of Conformity – Industrial Cyber Security Capability Product Capability Assessment acc. IEC 62443-4-2

- CP-8031/50: SL 2 (Security Level 2)
- CP-8012/12: SL 2 (Security Level 2)
- SICAM EGS: SL 2 (Security Level 2)

SIEMENS

Cybersecurity in the Power Grid
… calls for a Holistic Approach





SIEMENS

SICAM 8
SICAM S8000 - fulfills CIS benchmark level 2

SICAM S8000 achieves CIS benchmark Level 2

The Level 2 profile is considered to be “defense in depth” and is intended for environments where security is paramount

SICAM S8000 supports Secure Boot

Therefore, the host PC must be started in UEFI mode

Linux OS setup documentation “SICAM 8 Series, “Core Functions & Hardware, Manual”

SICAM S8000 – Linux system hardening is provided in “SICAM 8 Series, “Administrator Security, Manual”

SICAM A8000 适用于……

- 中压开关柜——优化设计的紧凑型设备，配备显示屏，可直接可视化
- 潮流控制
- 太阳能和风力发电场的并网
- 环网单元的控制与监测
- 物联网网关
- 铁路供电
- 通信网关

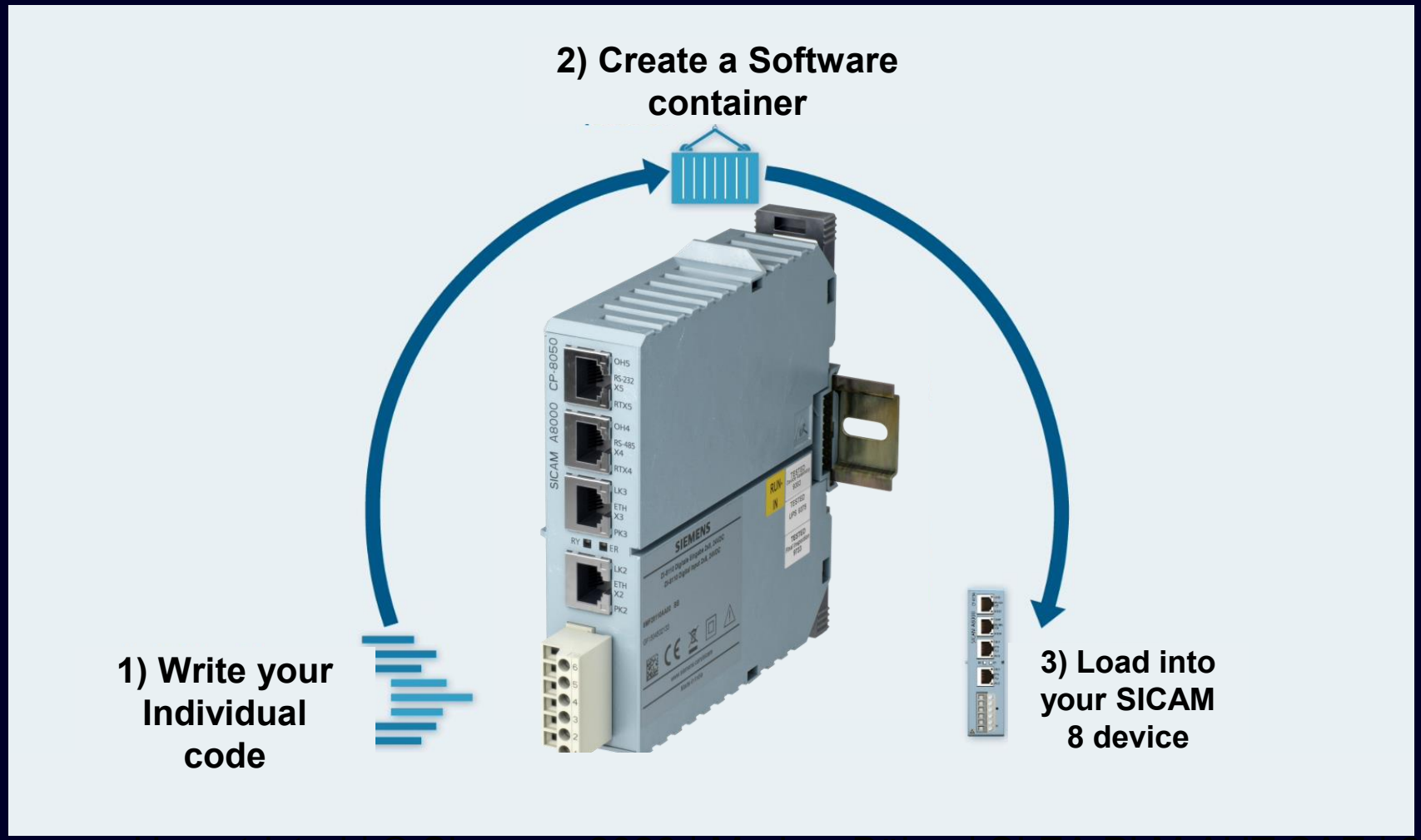

铁路供电


太阳能和
陆上风电场


配电

SIEMENS

SICAM 8
Build customer own Application by SIAPPs



SIAPP, more performance in only 3 basic steps

1) Write the code for your special requirement
2) Pack this code into a software container
3) Load this software container with SICAM Web into the A8000 processor module

With the A8000 features

- Rugged hardware
- Extensive RTU functionality
- Tested communication protocols

SIEMENS

SICAM 8
Hard facts on SIAPPs

Resource Limits per SIAPP / overall
- 300 MB RAM / 300 MB RAM
- 1 GB Flash / 1,5 GB Flash
- 2 processor cores / 2 processor cores

Platform restrictions
- CP-8050 / S8000: Max. 3 SIARS & 3 SIAPPS
- CP-8010/12/31 & EGS: Max. 1 SIAR & 1 SIAPP

Connectivity
- Edgedata API
- Exclusive physical ethernet port
- Virtual ethernet port

Additional Features
- Persistent memory for updates
- Parameter Interface via SICAM Device Manager
- Python access to edgedata API