技术推广中心
Technology Promotion Center

工业控制系统信息安全标准化现状

演讲人：李玉敏　教授/研究员

单位：机械工业仪器仪表综合技术经济研究所

日期：2014年10月24日　北京

技术推广中心
Technology Promotion Center

目 录

- 工业控制系统面临的形势
- 工控信息安全国际标准化概况
- 我国工控信息安全标准体系建设
- 面临的挑战与工作建议

面临的形势

技术推广中心 Technology Promotion Center

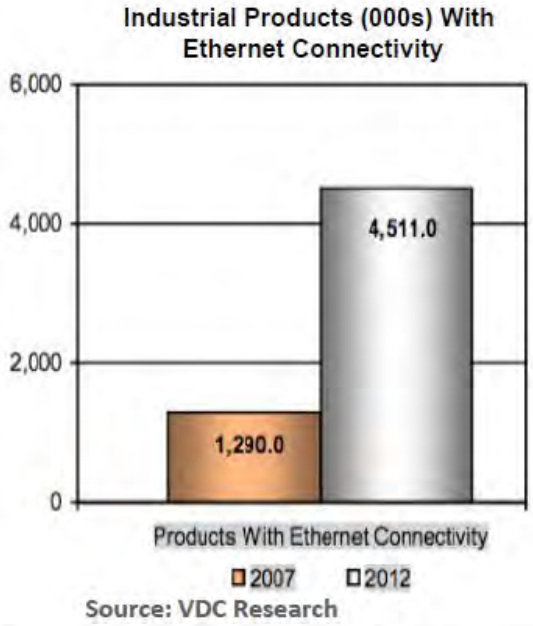
国民经济和社会运行的发展重点：

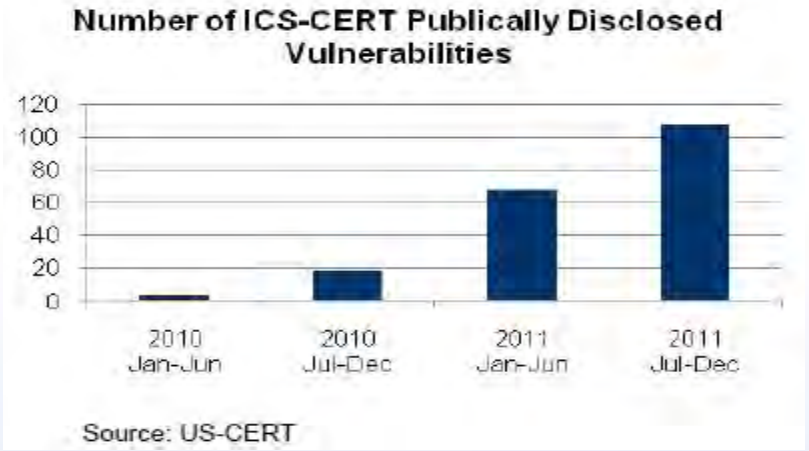
- 国家中长期科学和技术发展规划纲要（2006-2020年）
- 国家信息化领导小组关于加强信息安全保障工作的意见
- 国家信息安全科技发展规划要点
- 2011年10月，工信部印发《关于加强工控系统信息安全管理的通知》，《通知》明确，重点加强核设施、钢铁、有色、化工、石油石化、电力、天然气、先进制造、水利枢纽、环境保护、铁路、城市轨道交通、民航、城市供水供气供热以及其他与国计民生紧密相关领域的工控系统信息安全管理，落实安全管理要求。
- 2012年7月，为落实国办开展重点领域网络与信息安全检查行动，工信部开展了重点领域信息安全自查、抽查行动。

- 控制设备接入网络的数量越来越多
  - 工业控制设备接入网络的数量从2007年的130万增加到了2012年的450万，年增长28%（来源：VDC Research）

- 网络安全威胁越来越多
  - 美国计算机安全应急响应组US-CERT公开披露从2011年到2012年安全漏洞跃升了900% ！

- 安全忧患意识迅速增长
  - 调查显示，超过33%受访的工业管理者相信针对工业基础设施的网络攻击在上升
  - 其中40%预期在一年内企业将面临一场大型网络攻击 （来源：国际研究和策略中心Center for Strategic and International Studies ）

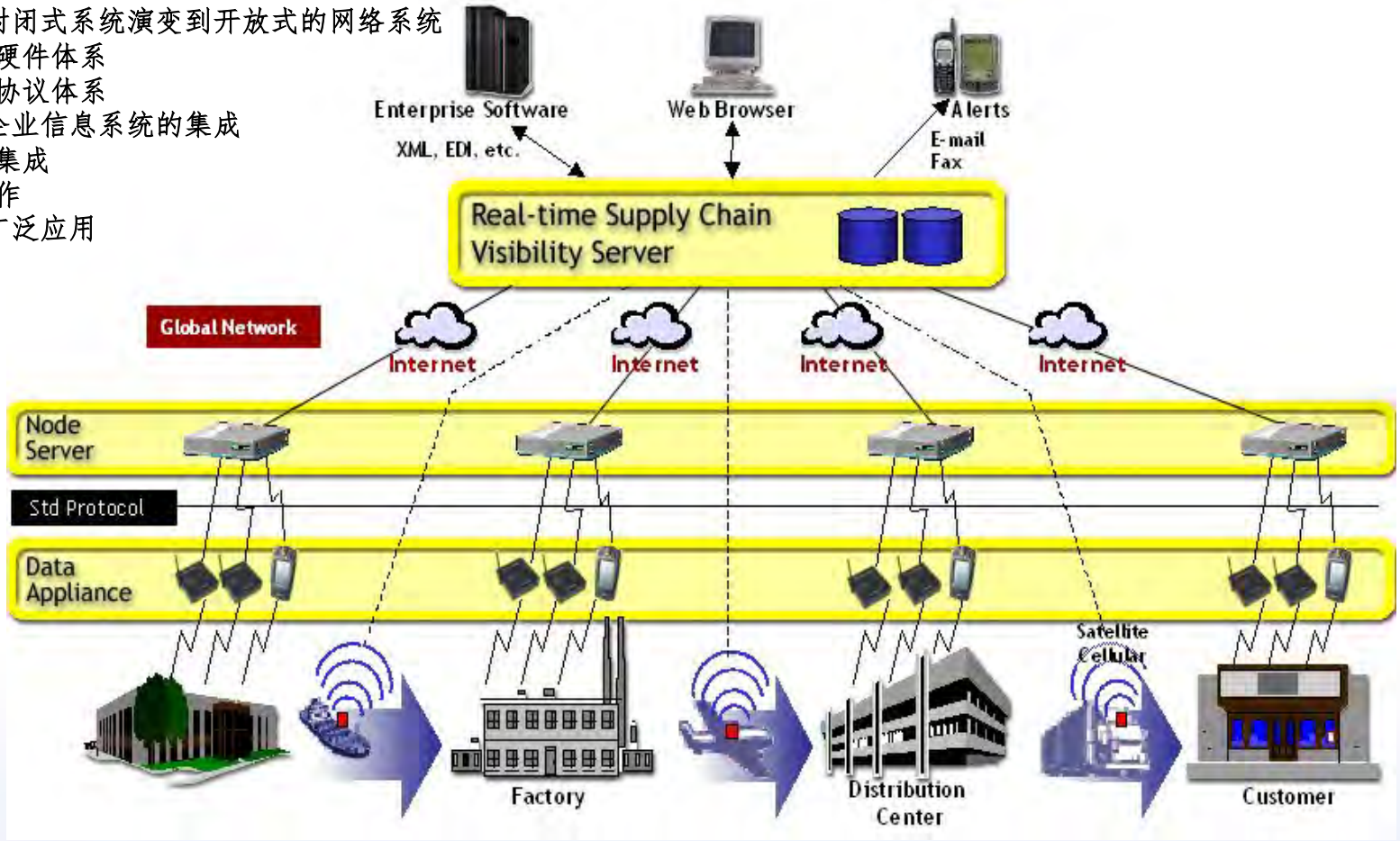




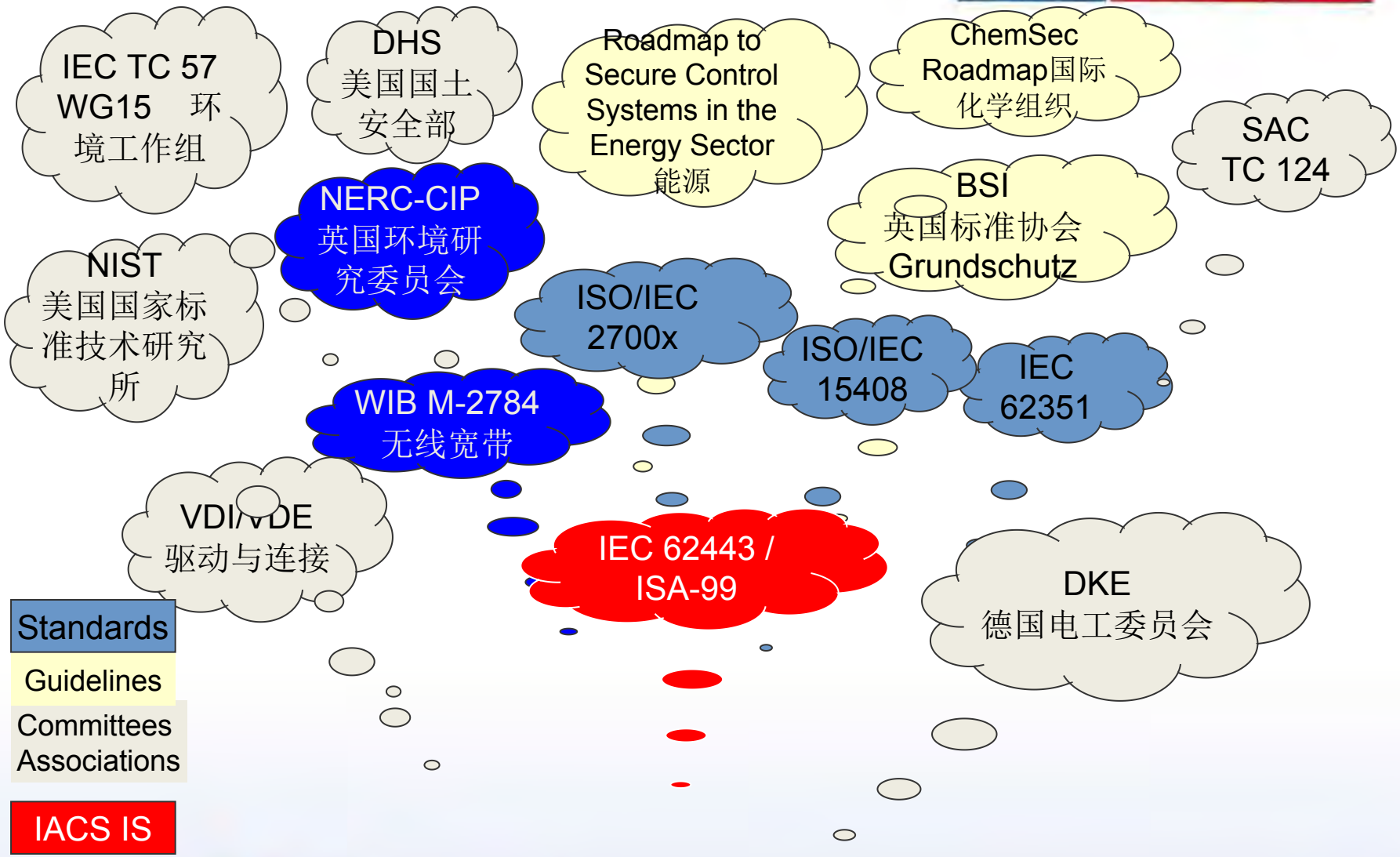
工控系统

工控系统发展趋势——数字化、网络化、智能化

- 从传统系统封闭式系统演变到开放式的网络系统
  - 开放的硬件体系
  - 开放的协议体系
- 过程控制和企业信息系统的集成
  - 供给链集成
  - 远程工作
- 无线技术的广泛应用

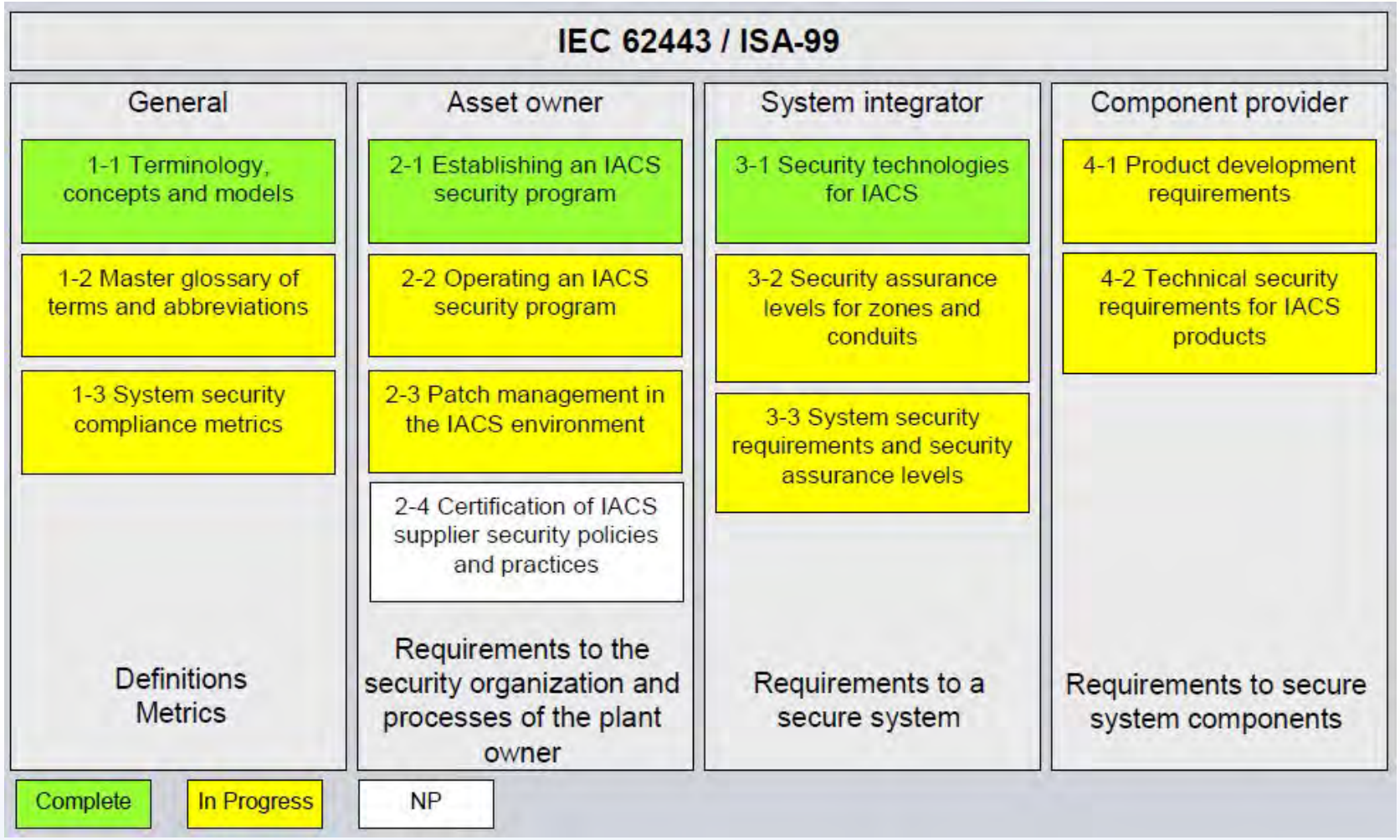


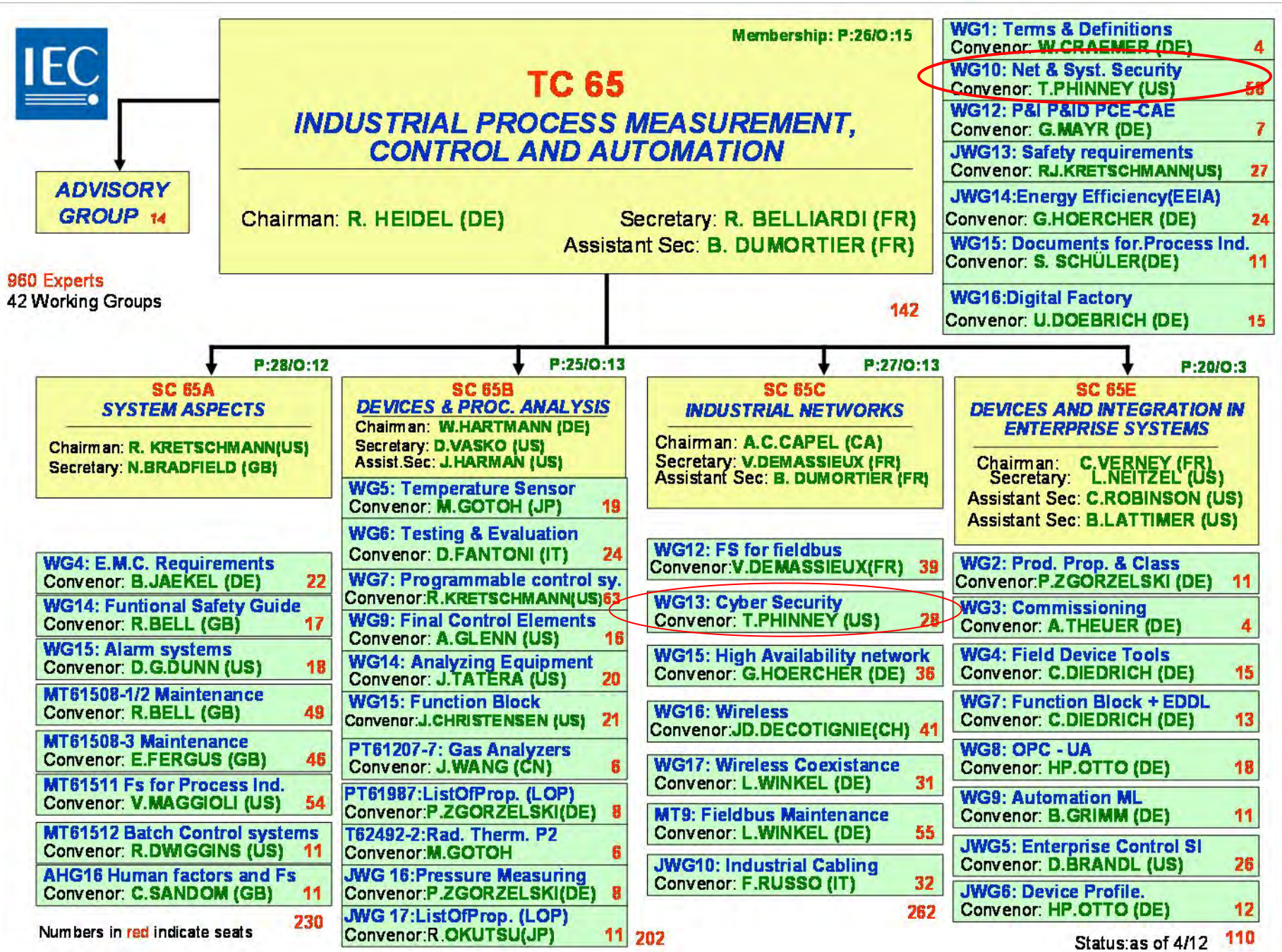
工控信息安全国际标准化



IEC62443系列标准框架

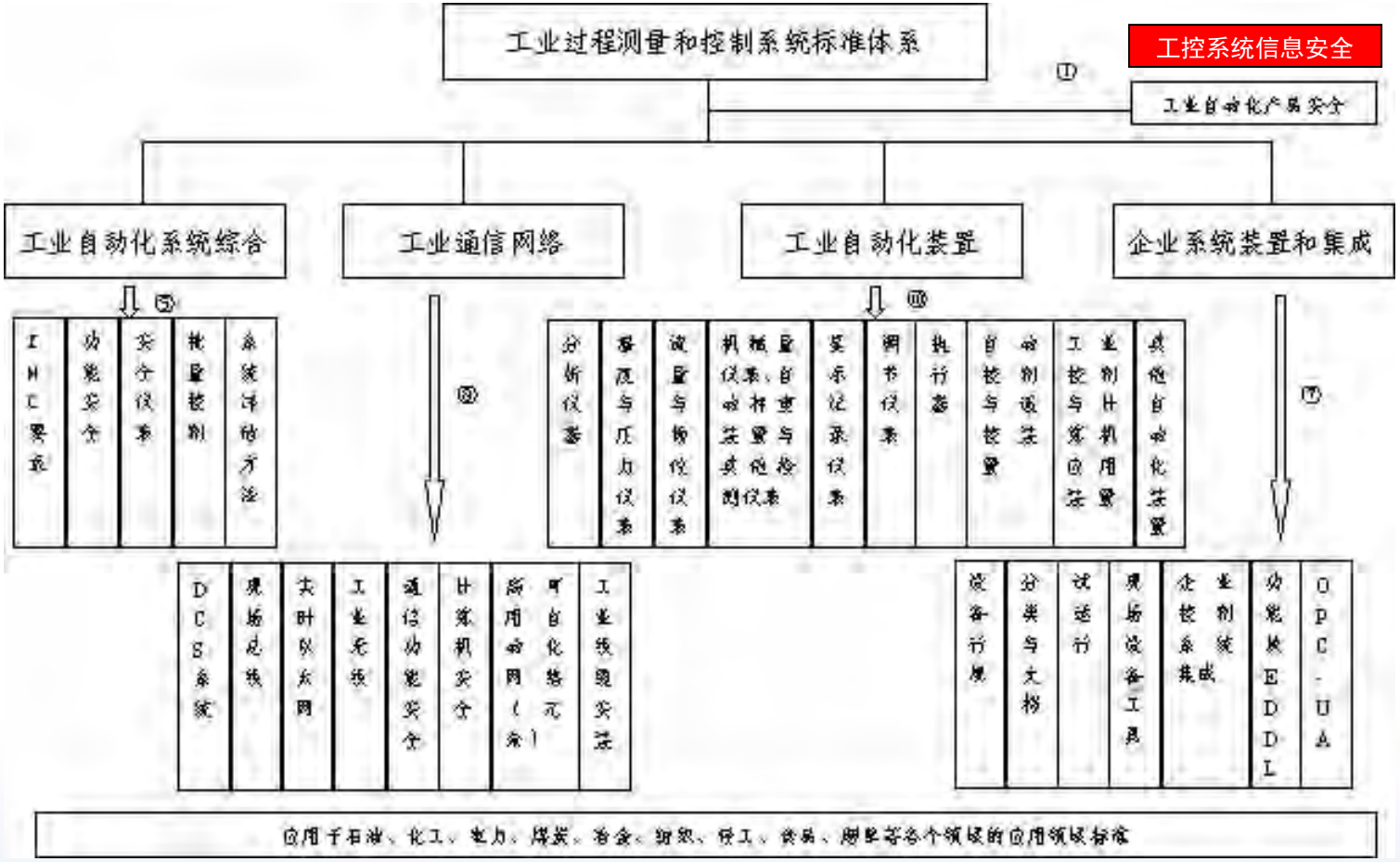
技术推广中心 Technology Promotion Center




Membership: P:26/O:15
TC 65
INDUSTRIAL PROCESS MEASUREMENT, CONTROL AND AUTOMATION
Chairman: R. HEIDEL (DE)
Secretary: R. BELLIARDI (FR)
Assistant Sec: B. DUMORTIER (FR)
ADVISORY GROUP 14
960 Experts
42 Working Groups
142
WG1: Terms & Definitions
Convenor: W.CRAEMER (DE) 4
WG10: Net & Syst. Security
Convenor: T.PHINNEY (US) 58
WG12: P&I P&ID PCE-CAE
Convenor: G.MAYR (DE) 7
JWG13: Safety requirements
Convenor: RJ.KRETSCHMANN(US) 27
JWG14:Energy Efficiency(EEIA)
Convenor: G.HOERCHER (DE) 24
WG15: Documents for.Process Ind.
Convenor: S. SCHÜLER(DE) 11
WG16:Digital Factory
Convenor: U.DOEBRICH (DE) 15
P:28/O:12
SC 65A
SYSTEM ASPECTS
Chairman: R. KRETSCHMANN(US)
Secretary: N.BRADFIELD (GB)
WG4: E.M.C. Requirements
Convenor: B.JAEKEL (DE) 22
WG14: Funtional Safety Guide
Convenor: R.BELL (GB) 17
WG15: Alarm systems
Convenor: D.G.DUNN (US) 18
MT61508-1/2 Maintenance
Convenor: R.BELL (GB) 49
MT61508-3 Maintenance
Convenor: E.FERGUS (GB) 46
MT61511 Fs for Process Ind.
Convenor: V.MAGGIOLI (US) 54
MT61512 Batch Control systems
Convenor: R.DWIGGINS (US) 11
AHG16 Human factors and Fs
Convenor: C.SANDOM (GB) 11
230
P:25/O:13
SC 65B
DEVICES & PROC. ANALYSIS
Chairman: W.HARTMANN (DE)
Secretary: D.VASKO (US)
Assist.Sec: J.HARMAN (US)
WG5: Temperature Sensor
Convenor: M.GOTOH (JP) 19
WG6: Testing & Evaluation
Convenor: D.FANTONI (IT) 24
WG7: Programmable control sy.
Convenor:R.KRETSCHMANN(US) 63
WG9: Final Control Elements
Convenor: A.GLENN (US) 16
WG14: Analyzing Equipment
Convenor: J.TATERA (US) 20
WG15: Function Block
Convenor:J.CHRISTENSEN (US) 21
PT61207-7: Gas Analyzers
Convenor: J.WANG (CN) 6
PT61987:ListOfProp. (LOP)
Convenor:P.ZGORZELSKI(DE) 8
T62492-2:Rad. Therm. P2
Convenor:M.GOTOH 6
JWG 16:Pressure Measuring
Convenor:P.ZGORZELSKI(DE) 8
JWG 17:ListOfProp. (LOP)
Convenor:R.OKUTSU(JP) 11
202
P:27/O:13
SC 65C
INDUSTRIAL NETWORKS
Chairman: A.C.CAPEL (CA)
Secretary: V.DEMASSIEUX (FR)
Assistant Sec: B. DUMORTIER (FR)
WG12: FS for fieldbus
Convenor:V.DEMASSIEUX(FR) 39
WG13: Cyber Security
Convenor: T.PHINNEY (US) 28
WG15: High Availability network
Convenor: G.HOERCHER (DE) 36
WG16: Wireless
Convenor:JD.DECOTIGNIE(CH) 41
WG17: Wireless Coexistance
Convenor: L.WINKEL (DE) 31
MT9: Fieldbus Maintenance
Convenor: L.WINKEL (DE) 55
JWG10: Industrial Cabling
Convenor: F.RUSSO (IT) 32
262
P:20/O:3
SC 65E
DEVICES AND INTEGRATION IN ENTERPRISE SYSTEMS
Chairman: C.VERNEY (FR)
Secretary: L.NEITZEL (US)
Assistant Sec: C.ROBINSON (US)
Assistant Sec: B.LATTIMER (US)
WG2: Prod. Prop. & Class
Convenor:P.ZGORZELSKI (DE) 11
WG3: Commissioning
Convenor: A.THEUER (DE) 4
WG4: Field Device Tools
Convenor: C.DIEDRICH (DE) 15
WG7: Function Block + EDDL
Convenor: C.DIEDRICH (DE) 13
WG8: OPC - UA
Convenor: HP.OTTO (DE) 18
WG9: Automation ML
Convenor: B.GRIMM (DE) 11
JWG5: Enterprise Control SI
Convenor: D.BRANDL (US) 26
JWG6: Device Profile.
Convenor: HP.OTTO (DE) 12
Numbers in red indicate seats
Status:as of 4/12
110

我国的标准体系

技术推广中心 Technology Promotion Center



机械工业仪器仪表综合技术经济研究所

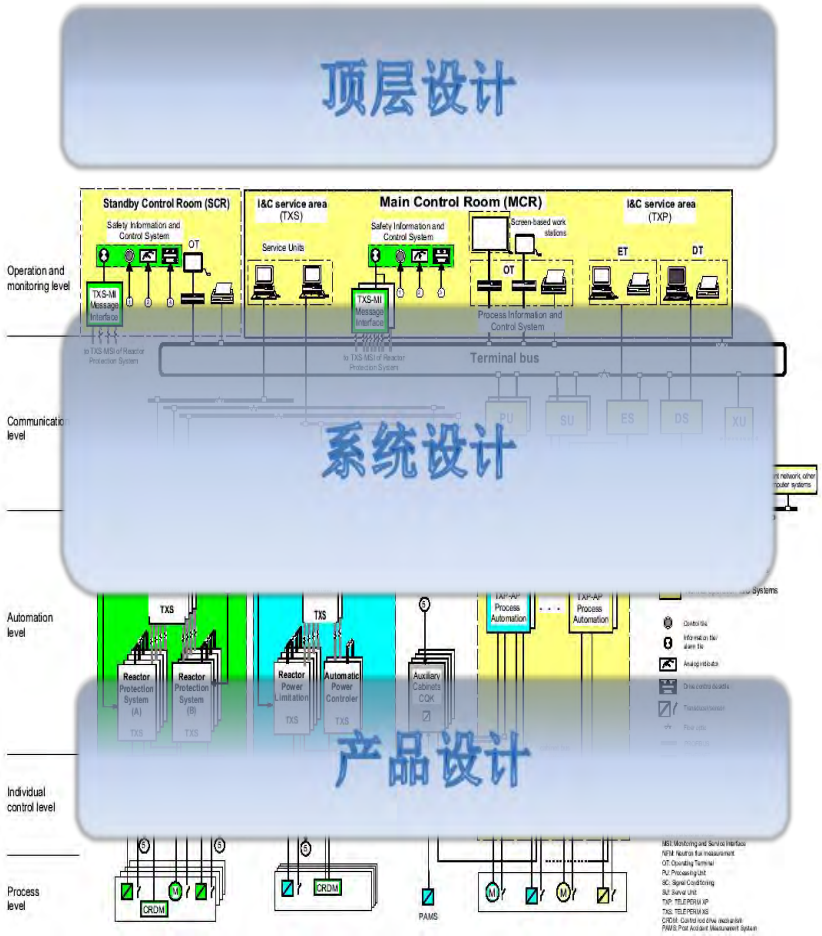
信息安全标准体系

■ 联合相关标委会，制定11项国家/行业标准，初步建立了系统级的安全要求标准体系：

» 顶层设计：建立了基于技术与管理方法的评估规范和验收规范；

» 系统设计：建立了DCS、现场总线、PLC系统安全设计规范；

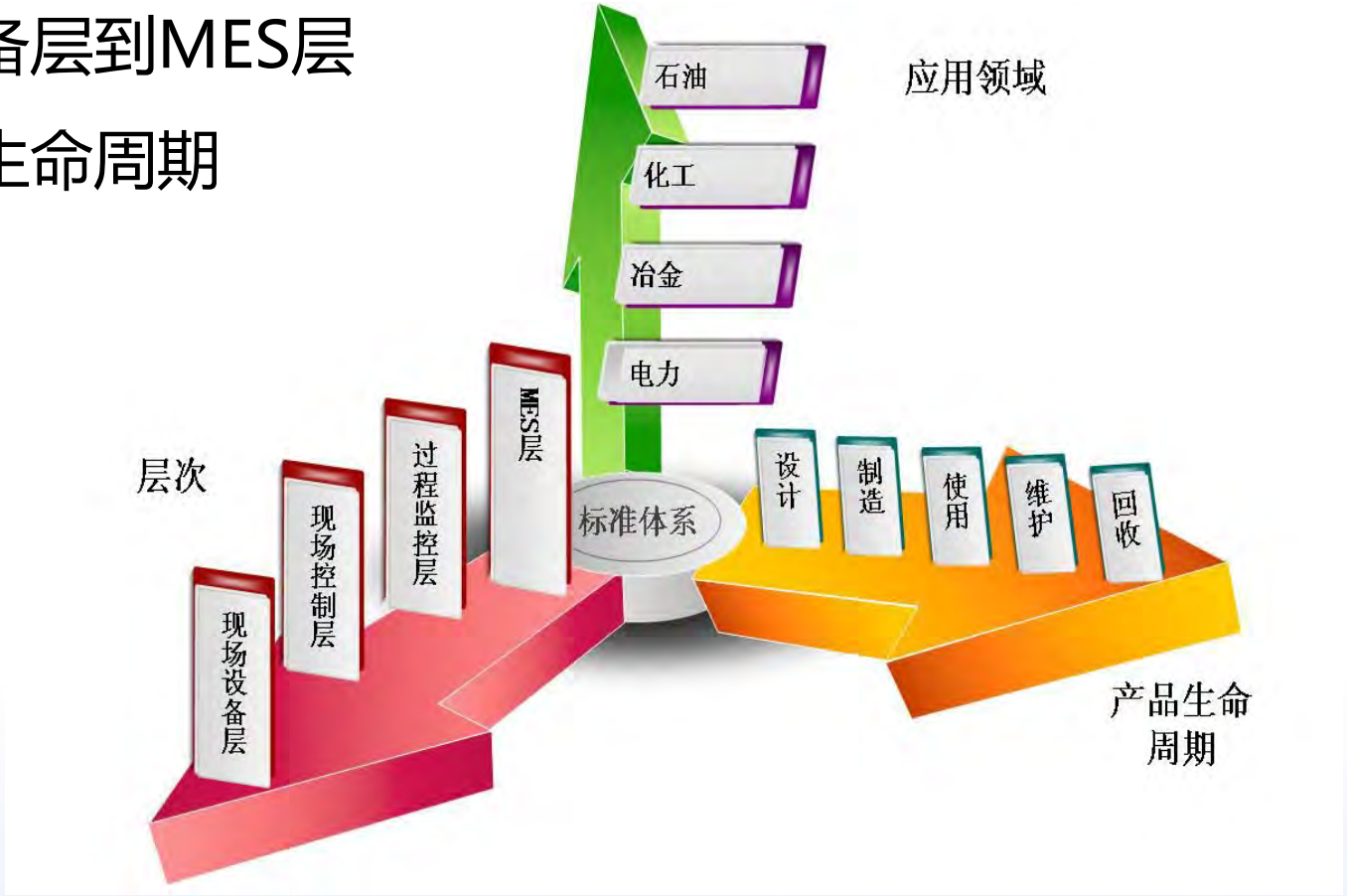
» 产品设计：即将建立基于嵌入式系统的产品安全规范。



信息安全标准体系

技术推广中心 Technology Promotion Center

- 领域：适应工控系统所有应用领域
- 层次：现场设备层到MES层
- 系统：产品全生命周期



我国标准研制进程

技术推广中心 Technology Promotion Center

已发布国家标准（2项）	国家标准计划项目（6项）	已发布行业标准（3项）
• GB/T 30976.1-2014 工控系统信息安全 第1部分：评估规范 • GB/T 30976.2-2014 工控系统信息安全 第2部分：验收规范	• 20120829-T-604 工业通信网络 网络和系统安全 第2-1部分（ 等同 IEC 62443-2-1：2010）（10月送审） • 20130783-T-604 集散控制系统（DCS）安全防护标准（10月送审） • 20130784-T-604 集散控制系统（DCS）安全管理标准（10月送审） • 20130785-T-604 集散控制系统（DCS）安全评估标准（10月送审） • 20130786-T-604 集散控制系统（DCS） 风险与脆弱性检测标准（10月送审） • 20130787-T-604 可编程逻辑控制器（PLC） 安全要求（10月送审）	• JB/T 11960-2014 工业过程测量和控制安全 网络和系统安全（IEC/TR62443-3：2008） • JB/T 11961-2014 工业通信网络 网络和系统安全 术语、概念和模型 （IEC /TS62443-1-1：2009） • JB/T 11962-2014 工业通信网络 网络和系统安全 工业自动化和控制系统信息安全技术（IEC/TR62443-3-1：2009）

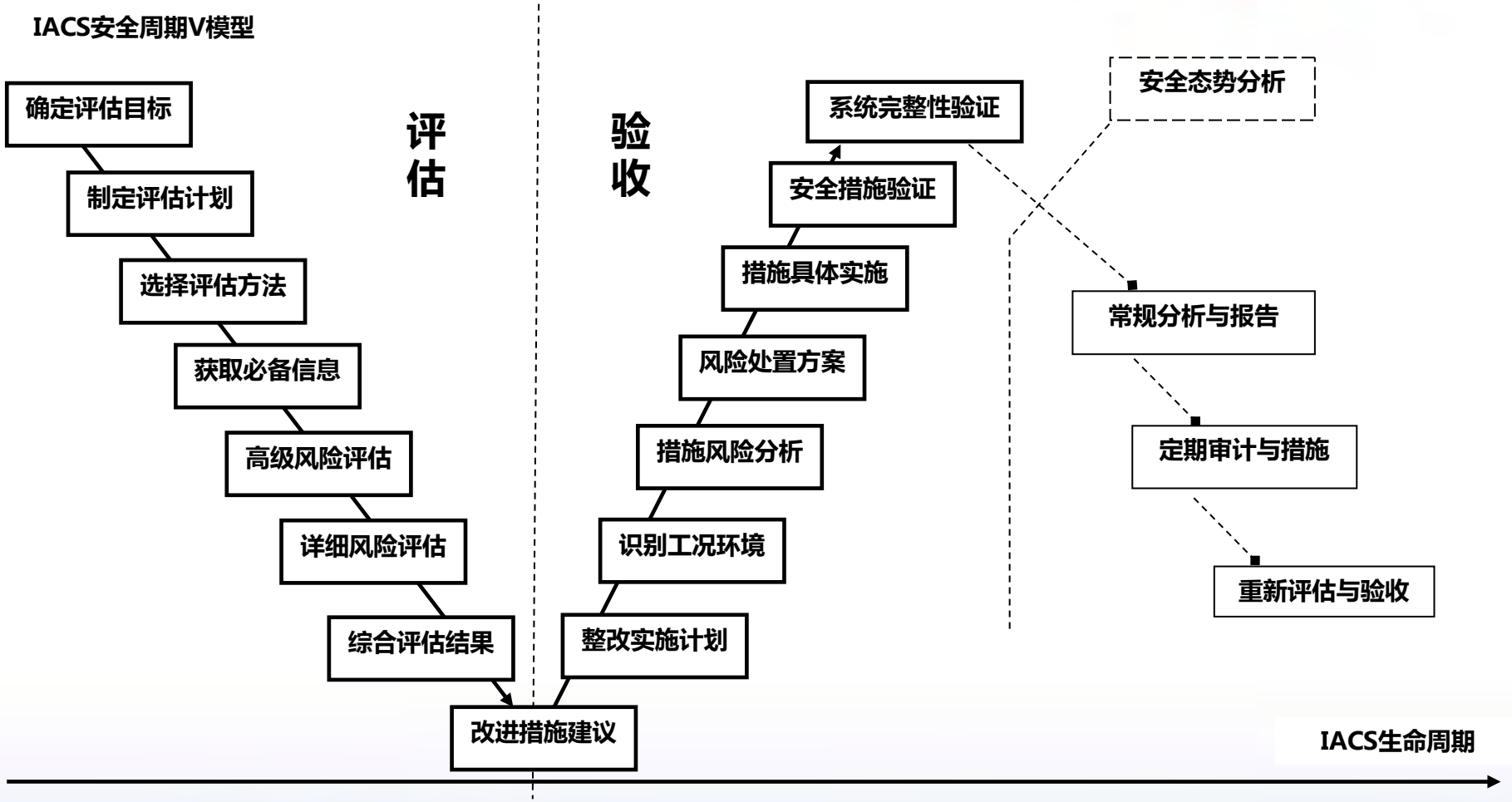
信息安全等级

技术推广中心 Technology Promotion Center

- 管理等级
  - »基于ISO27002的管理要求；
  - »基于WIB；
  - »三级划分；
- 系统能力等级
  - »基于IEC62443-3-3技术要求；
  - »四级划分；
- 信息安全等级
  - »管理要求与技术要求加权；
  - »四级划分。

系统能力等级 信息安全等级 管理等级	CL1	CL2	CL3	CL4
ML1	SL1	SL1	SL1	SL1
ML2	SL1	SL2	SL2	SL3
ML3	SL1	SL2	SL3	SL4

IACS安全周期V模型



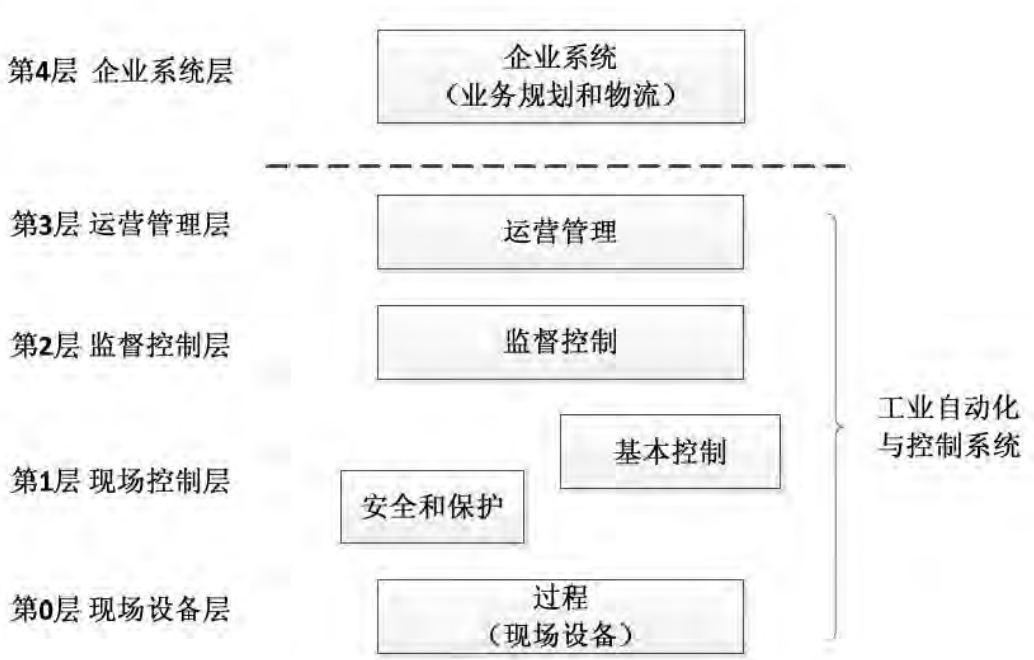
PLC系统信息安全要求

技术推广中心 Technology Promotion Center

» 定义了从现场设备层到运营管理层的信息安全要求。

» 主要描述风险内容、安全技术要求、安全管理要求、检测与验收等。

» 包括系统生命周期内的设计开发、安装、运行维护、退出使用等各阶段与系统相关的所有活动。



DCS系统信息安全要求

技术推广中心 Technology Promotion Center

安全防护标准中定义了集散控制系统在运行和维护过程中应具备的安全能力和防护技术要求

安全管理标准定义了集散控制系统在运行和维护过程中应具备的安全管理要点和防护管理要求

风险与脆弱性检测标准定义了集散控制系统在运行和维护过程中潜在系统脆弱性和安全风险的检测内容和测试方法

安全评估标准定义了集散控制系统在运行和维护过程中对系统技术防护能力和安全管理有效性的评估过程和方法。

面临的挑战

- 安全防控意识应当加强
- 建立政策+管理+技术的模式
- 测试技术和测试平台缺乏
- 国外机构主导安全的评估

—— 安全命脉掌握在发达国家

工作建议

技术推广中心 Technology Promotion Center

- 对重大设施、装备等进行风险评估，明确重大危险源和生产工艺，开展安全分级管理，加快国家标准和相关规范制定，建立认证评估体系。
- 积极跟踪和参与国际认证规范的制定，从设计起步阶段反映我国产业需求，体现我国工业安全意志。
- 建立国家级的工业安全测评中心或实验室
- 加速人才队伍培养，全面掌握工业控制和相关安全知识 ……

特别对于工业信息安全：不可能实现一个认证全球通行

谢谢！