工控信息安全——国际标准概况及我国的体系建设

演讲人：欧阳劲松

职务：机械工业仪器仪表综合技术经济研究所（ITEI）所长

全国工业过程测量控制和自动化标准化技术委员会（SAC/TC124）副主任委员

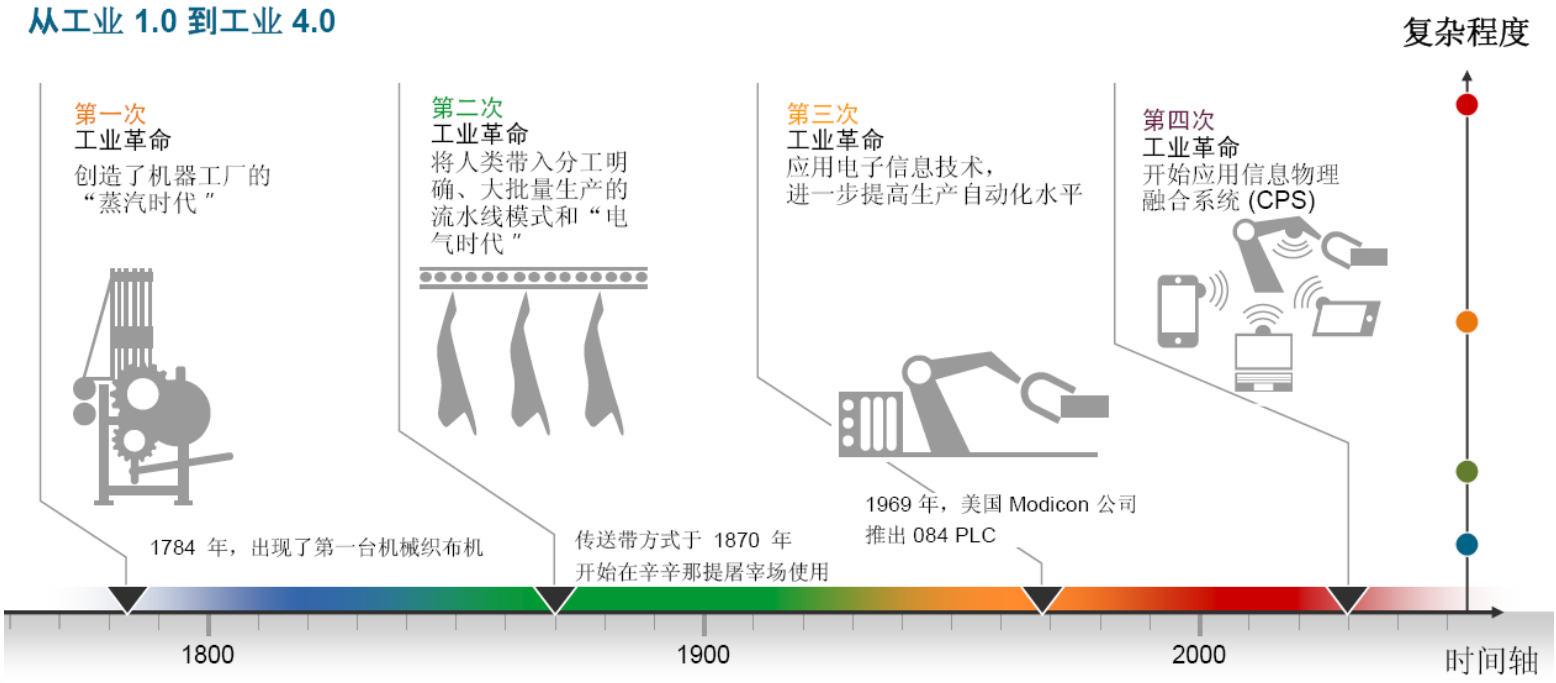
日期：2014年9月24日

目 录

- 工控技术发展与信息安全势态
- 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

技术发展需求

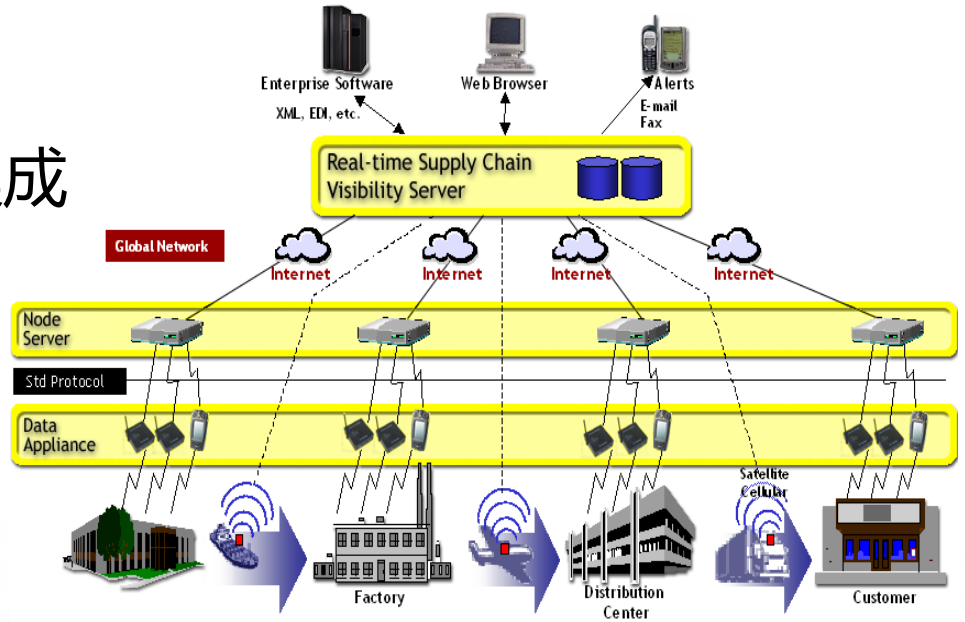
- 以智能制造为主导的第四次工业革命正在兴起



技术发展需求

工控系统发展的特点——
全球互联、嵌入式智能、自组织

- 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
  - 企业间协同
- 无线技术的广泛应用



安全势态

工控系统信息安全势态：

2010年	2011年	2012年
伊朗政府核电站员工感染Stuxnet病毒，严重威胁核反应堆安全运营	黑客入侵数据采集与监控系统，使美国伊利诺伊州城市供水系统的供水泵遭到破坏	两座美国电厂遭USB病毒攻击，感染了每个工厂的工控系统，可被窃取数据
	微软警告称最新发现的“Duqu”病毒可从工业控制系统制造商收集情报数据	发现攻击多个中东国家的恶意程序Flame火焰病毒，它能收集各行业的敏感信息

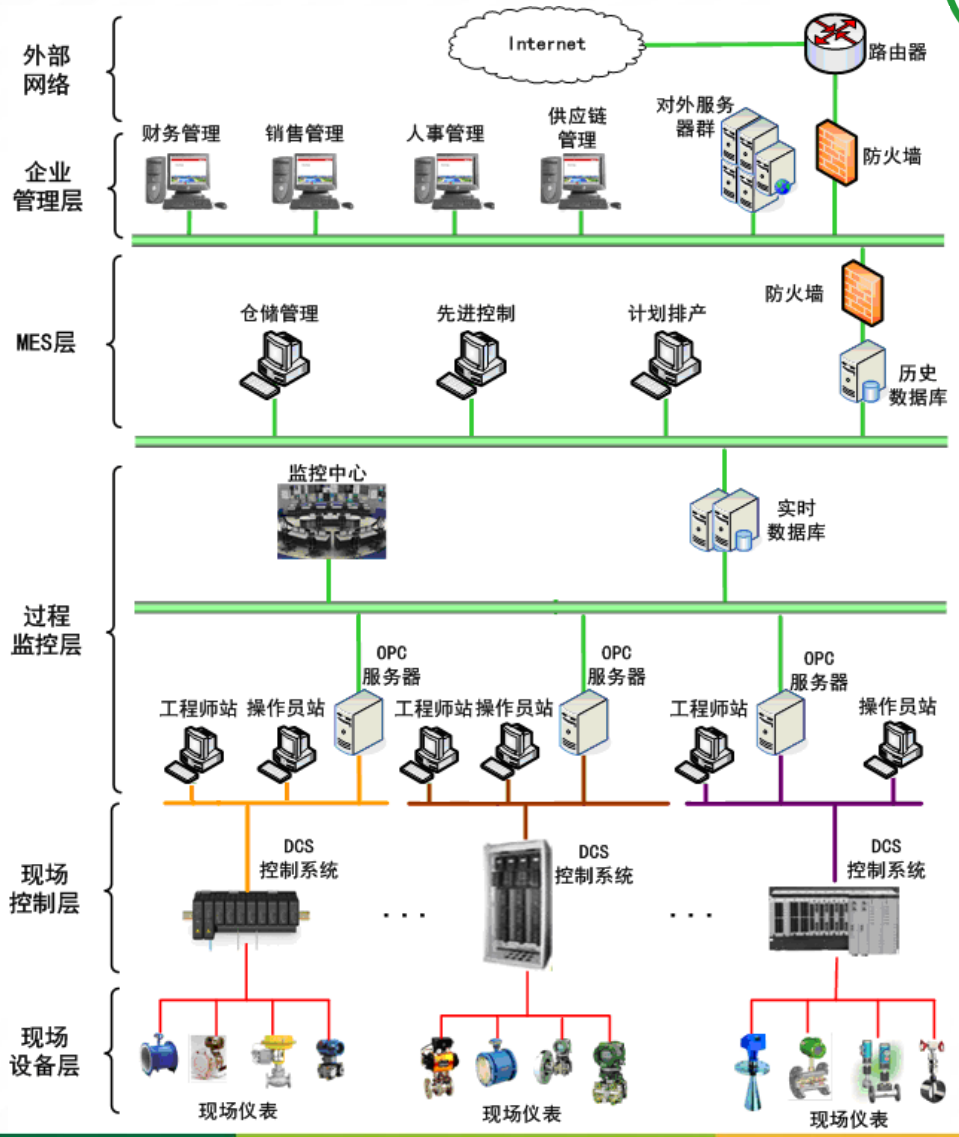
我国：2010年齐鲁石化、2011年大庆石化炼油厂，某装置控制系统分别感染Conficker蠕虫病毒，都造成控制系统服务器与控制器通讯不同程度地中断

企业分层模型

以MES制造执行系统层分界

— 向上为传统IT领域

— 向下为工控领域



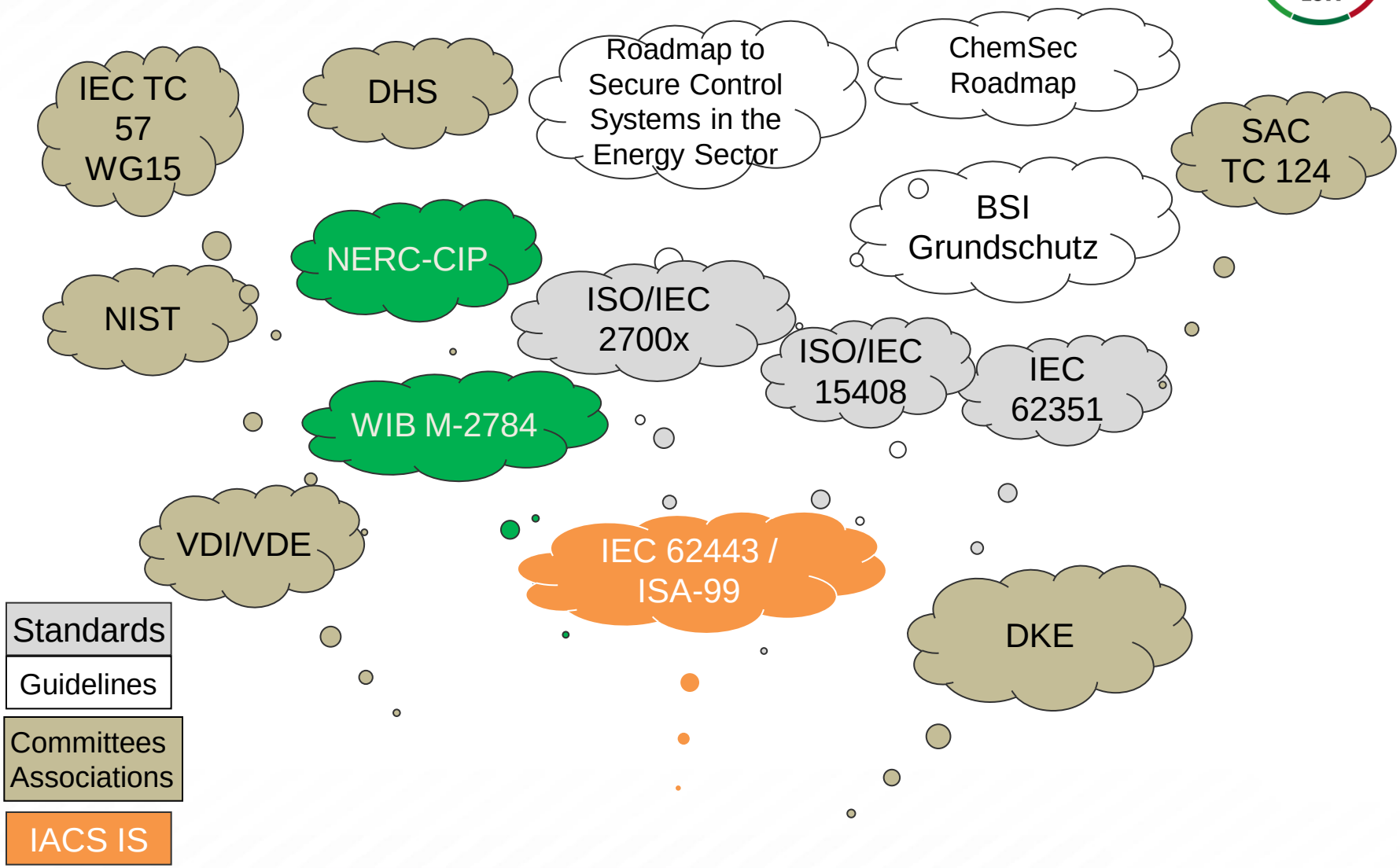
IT系统与工控系统的需求比较

	IT系统	工控系统
可用性	允许短时间/周期性的间断或维护	要求24h/7d/365d模式的可用性
时间敏感性	允许一定时延	要求实时响应
系统生命周期	3-5年	5-20年
信息安全意识及准备	较好	没有基础
保密性	较高	要求较低
设备类型	较少	较多
无线技术应用	很多	刚刚起步

传统信息系统：保密性—完整性—可用性

工控系统：可用性—完整性—保密性

信息安全标准


IEC TC 57 WG15
DHS
Roadmap to Secure Control Systems in the Energy Sector
ChemSec Roadmap
SAC TC 124
BSI Grundschutz
NERC-CIP
NIST
ISO/IEC 2700x
ISO/IEC 15408
IEC 62351
WIB M-2784
VDI/VDE
IEC 62443 / ISA-99
DKE
Standards
Guidelines
Committees Associations
IACS IS

国际上主要的工控信息安全标准

国际标准

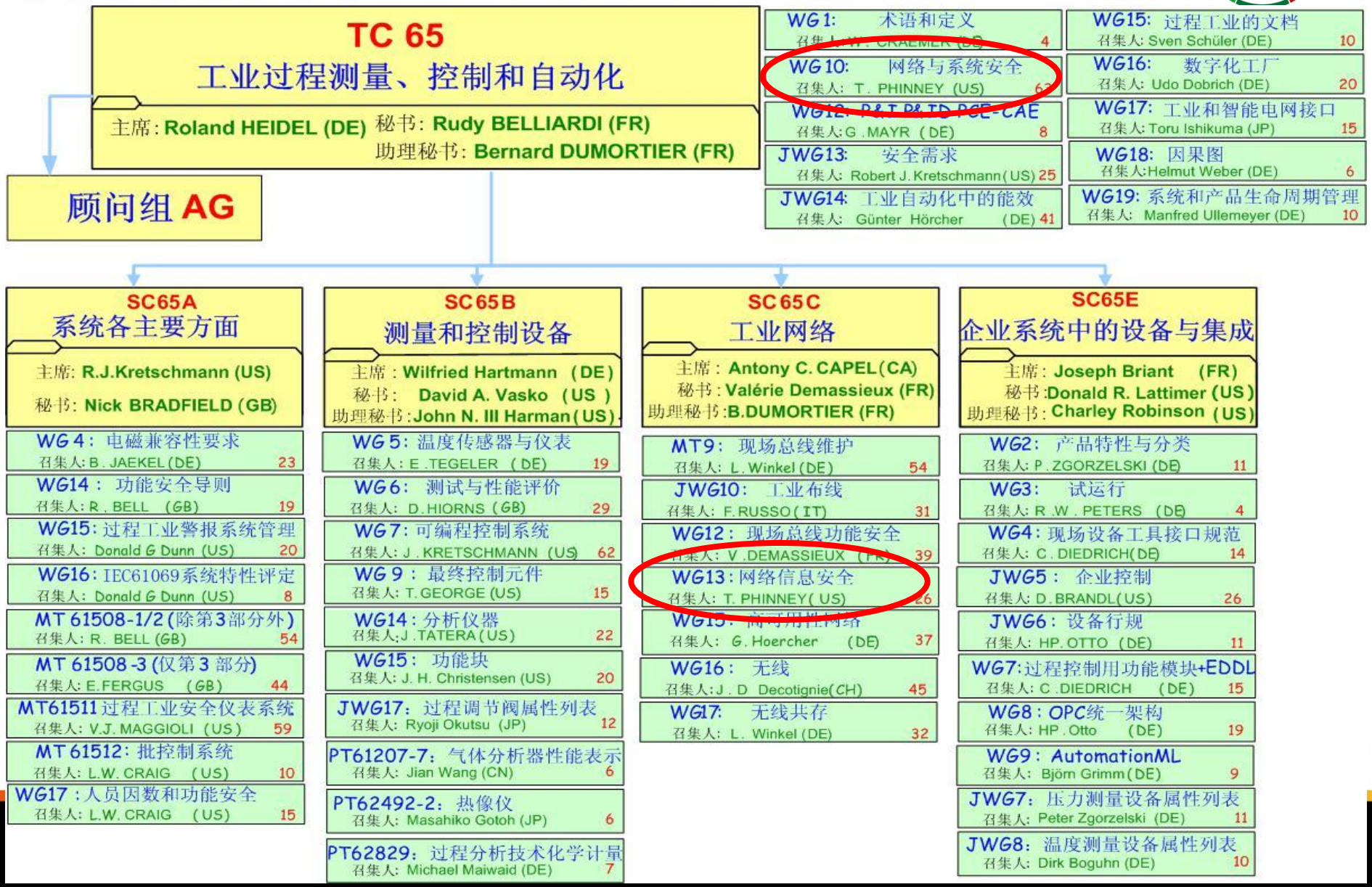
- IEC 62443《工业过程测量、控制和自动化　网络与系统信息安全》
- IEC 62351《电力系统管理与相关信息交互　数据和通信信息安全》
- ISO/IEC 27000《信息安全管理系统》

国家及技术组织标准

- NIST: SP800-82《工业控制系统信息安全指南》
- WIB M2784《过程控制领域中对供应商的信息安全要求》
- NERC CIP《网络信息安全　系统信息安全管理》
- ISA99: 已转为IEC 62443
- ……

WIB：石油天然气用户组织（荷兰）　　NERC：北美电力可靠性公司（美国）

IEC/TC65组织结构图



IEC/TC65/WG10 网络和系统安全

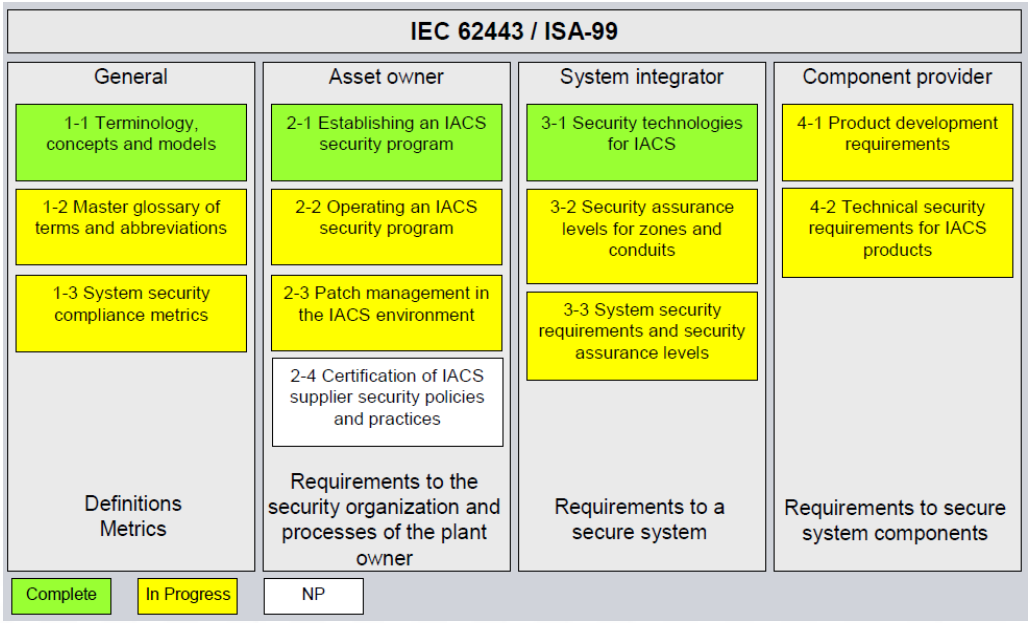
- 2007年决定成立IEC/TC65/WG10与ISA99联合工作组
- IEC 62443《工业过程测量、控制和自动化　网络与系统信息安全》

共包括12个部分，其中4个部分已发布，4个部分在投票或制定过程中

- 第1部分　概述
- 第2部分　对工厂业主和过程的要求
- 第3部分　对安全系统的要求
- 第4部分　对部件的要求

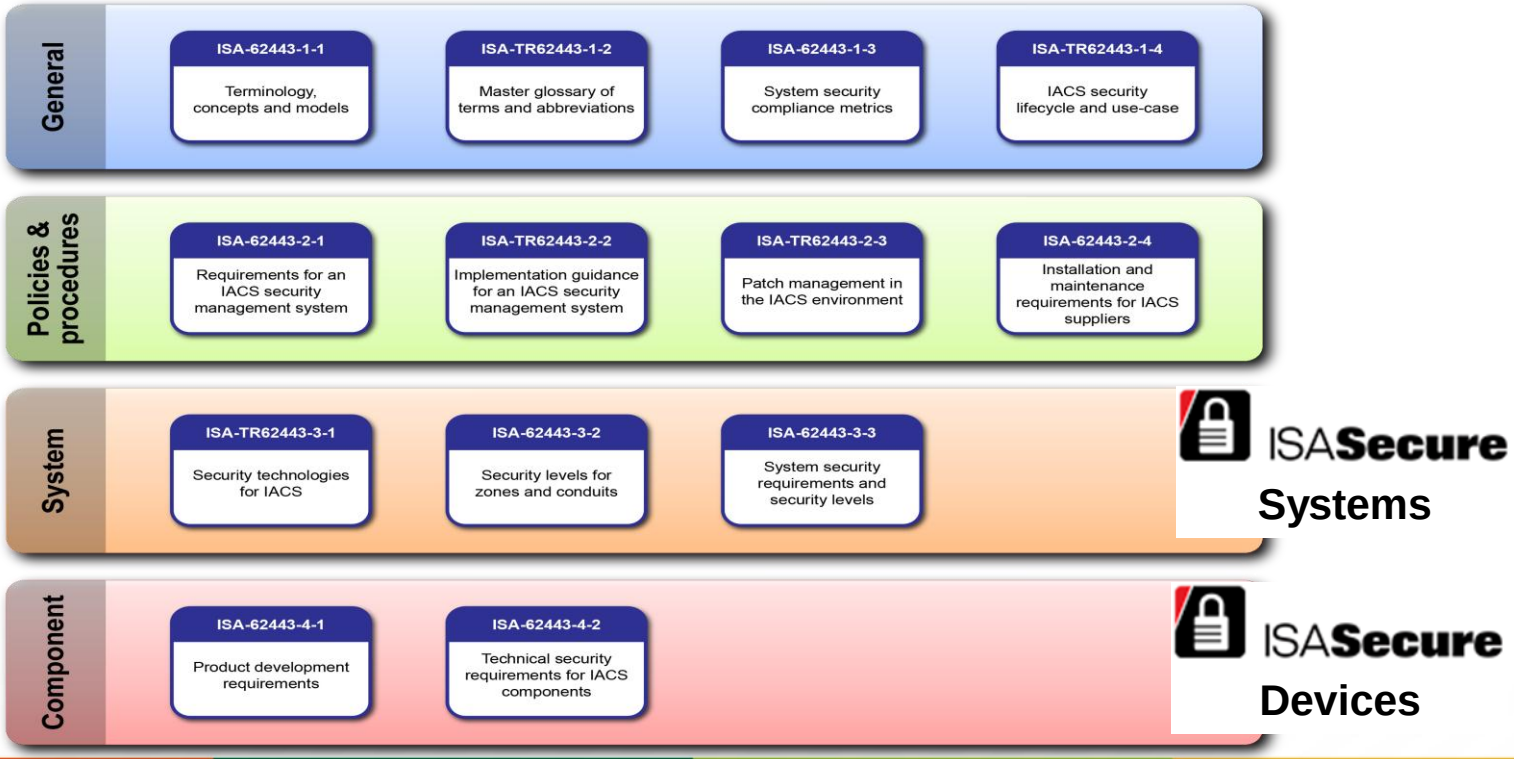
已在安全技术要求方面给出SL分级

SL: Security Level



ISA Secure认证

- 2007年，成立ISA安全符合性研究院ISCI（Security Compliance Institute）对标准的符合性进行认证
- Honeywell（3款）、RTP（1款）、横河（2款）、日立（1款）产品已通过ISASecure认证



ISA Secure嵌入式设备测试

嵌入式设备安全保证 (EDSA)

软件开发安全评估 (SDSA)

功能性安全评估(FSA)

通信健壮性测试(CRT)

检测和避免系统设计错误

- 审核供应商的软件开发和维护程序
- 确保组织机构遵照稳定和安全的软件开发程序

检测执行错误 / 疏忽

- 按照目标安全等级的要求对组件的安全功能进行审核
- 确保产品能够达到安全功能要求

鉴别网络和设备缺陷

- 根据通信健壮性要求测试组件的通信健壮性
- 基于4层OSI参考模型进行缺陷测试

最新进展

- IEC/TC65发布65/569/DC，建立一个协调Safety和Security的特别工作组（AD-HOC Group），以提出建议和新项目提案

工作组的研究内容包括：

1、现有相关标准；

2、 Safety和Security的区别；

3、 Safety和Security的共性；

4、协调Safety和Security的限制；

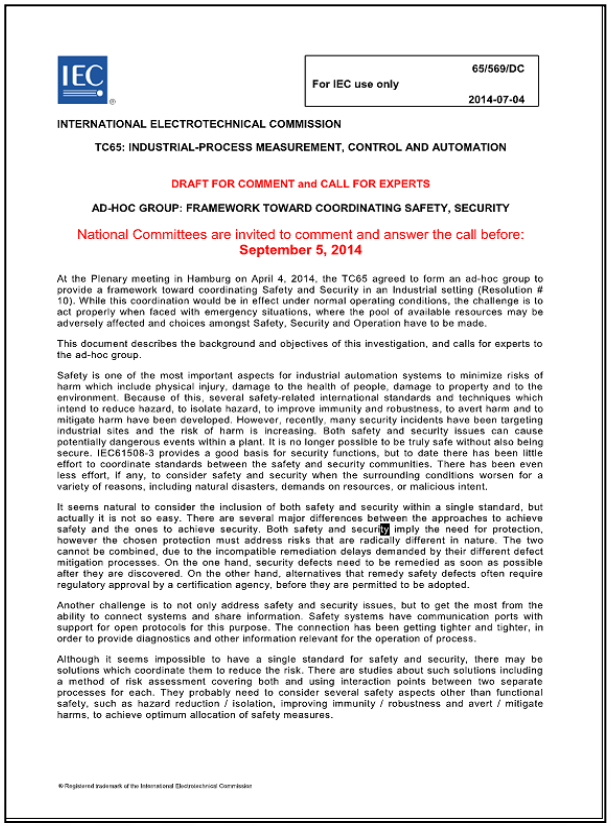
5、可能的协调方法；

6、紧急情况下的权衡与取舍；

7、建议和新项目提案的范围。

现向各国征集意见并召集专家（截至9月5日）

第一次会议定于2014.10.28-29 德国法兰克福



IEC

For IEC use only

65/569/DC

2014-07-04

INTERNATIONAL ELECTROTECHNICAL COMMISSION

TC65: INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION

DRAFT FOR COMMENT and CALL FOR EXPERTS

AD-HOC GROUP: FRAMEWORK TOWARD COORDINATING SAFETY, SECURITY

National Committees are invited to comment and answer the call before:
September 5, 2014

At the Plenary meeting in Hamburg on April 4, 2014, the TC65 agreed to form an ad-hoc group to provide a framework toward coordinating Safety and Security in an Industrial setting (Resolution # 10). While this coordination would be in effect under normal operating conditions, the challenge is to act properly when faced with emergency situations, where the pool of available resources may be adversely affected and choices amongst Safety, Security and Operation have to be made.

This document describes the background and objectives of this investigation, and calls for experts to the ad-hoc group.

Safety is one of the most important aspects for industrial automation systems to minimize risks of harm which include physical injury, damage to the health of people, damage to property and to the environment. Because of this, several safety-related international standards and techniques which intend to reduce hazard, to isolate hazard, to improve immunity and robustness, to avert harm and to mitigate harm have been developed. However, recently, many security incidents have been targeting industrial sites and the risk of harm is increasing. Both safety and security issues can cause potentially dangerous events within a plant. It is no longer possible to be truly safe without also being secure. IEC61508-3 provides a good basis for security functions, but to date there has been little effort to coordinate standards between the safety and security communities. There has been even less effort, if any, to consider safety and security when the surrounding conditions worsen for a variety of reasons, including natural disasters, demands on resources, or malicious intent.

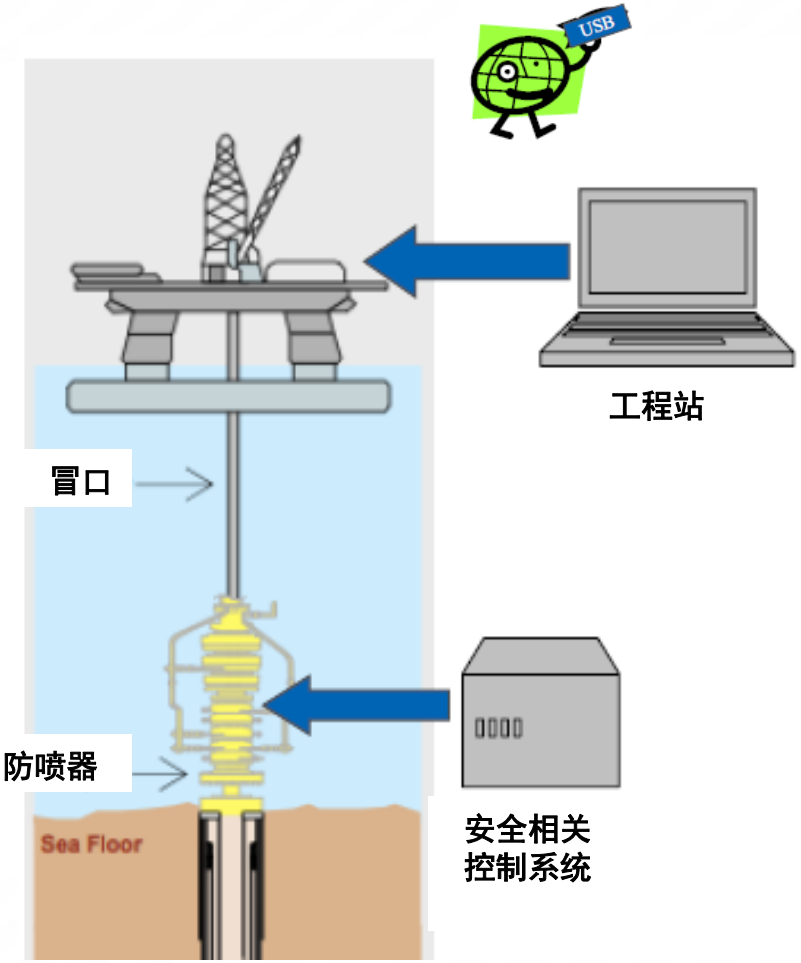
It seems natural to consider the inclusion of both safety and security within a single standard, but actually it is not so easy. There are several major differences between the approaches to achieve safety and the ones to achieve security. Both safety and security imply the need for protection, however the chosen protection must address risks that are radically different in nature. The two cannot be combined, due to the incompatible remediation delays demanded by their different defect mitigation processes. On the one hand, security defects need to be remedied as soon as possible after they are discovered. On the other hand, alternatives that remedy safety defects often require regulatory approval by a certification agency, before they are permitted to be adopted.

Another challenge is to not only address safety and security issues, but to get the most from the ability to connect systems and share information. Safety systems have communication ports with support for open protocols for this purpose. The connection has been getting tighter and tighter, in order to provide diagnostics and other information relevant for the operation of process.

Although it seems impossible to have a single standard for safety and security, there may be solutions which coordinate them to reduce the risk. There are studies about such solutions including a method of risk assessment covering both and using interaction points between two separate processes for each. They probably need to consider several safety aspects other than functional safety, such as hazard reduction / isolation, improving immunity / robustness and avert / mitigate harms, to achieve optimum allocation of safety measures.

®Registered trademark of the International Electrotechnical Commission

案例分析： Safety & Security



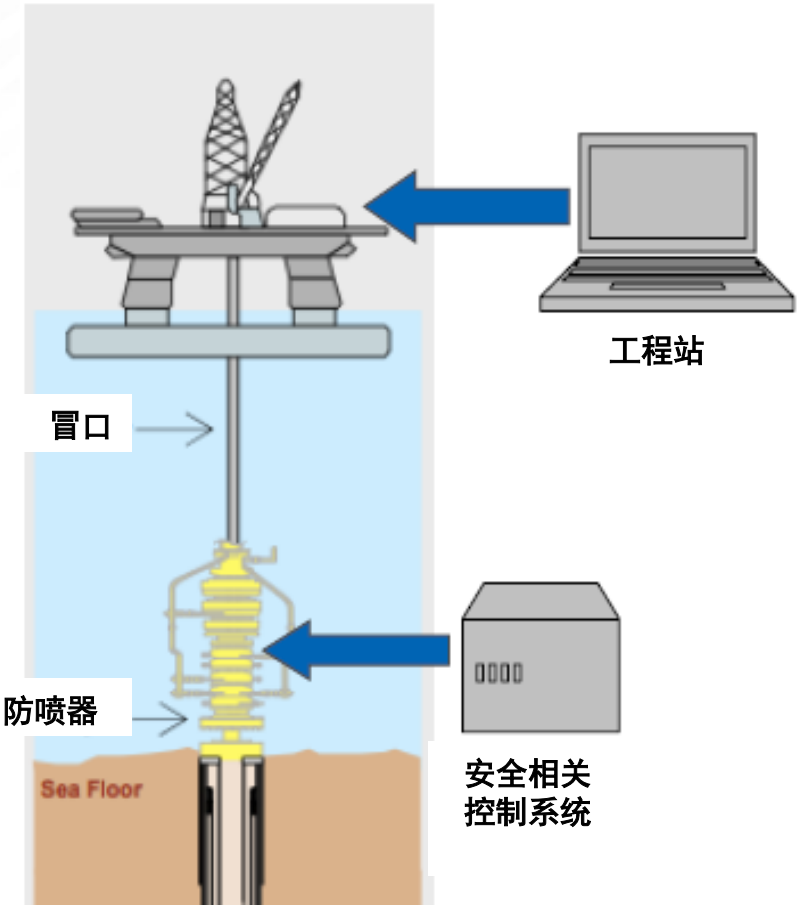
安全相关系统功能失效

通过控制系统或工程进行攻击

防喷器功能失效

钻井平台事故

图片来源：BP石油公司研究报告



■ 信息安全

攻击者发现新的漏洞、设计缺陷或是之前没有认为是漏洞的属性。

- 措施：

——深度防御

——工作管理系统（ “process” ）

■ 功能安全

元件的随机硬件失效和系统性失效（电磁阀卡住和电池没电）

- 措施

——用概率预测控制随机硬件失效

——用寿命周期管理系统和技术避免系统失效

——系统容错能力

工控系统自身特点决定：需要协调分析功能安全和信息安全

(尤其是风险分析和定义要求上)

IECEE - 工业自动化认证INDAT

（IEC电工产品合格测试与认证组织）

- **工业设备电气安全（物理安全）**

IEC 61010-2-201: 控制系统：例如, PLC, DCS, PAC
IEC 61010-2-20a: 独立电源
IEC 61010-2-20b: 包含运动的执行器：例如，旋转，线性阀门
IEC 61010-2-20c: 不包含运动的执行器
IEC 61010-2-20d: 人机接口

- **功能安全**

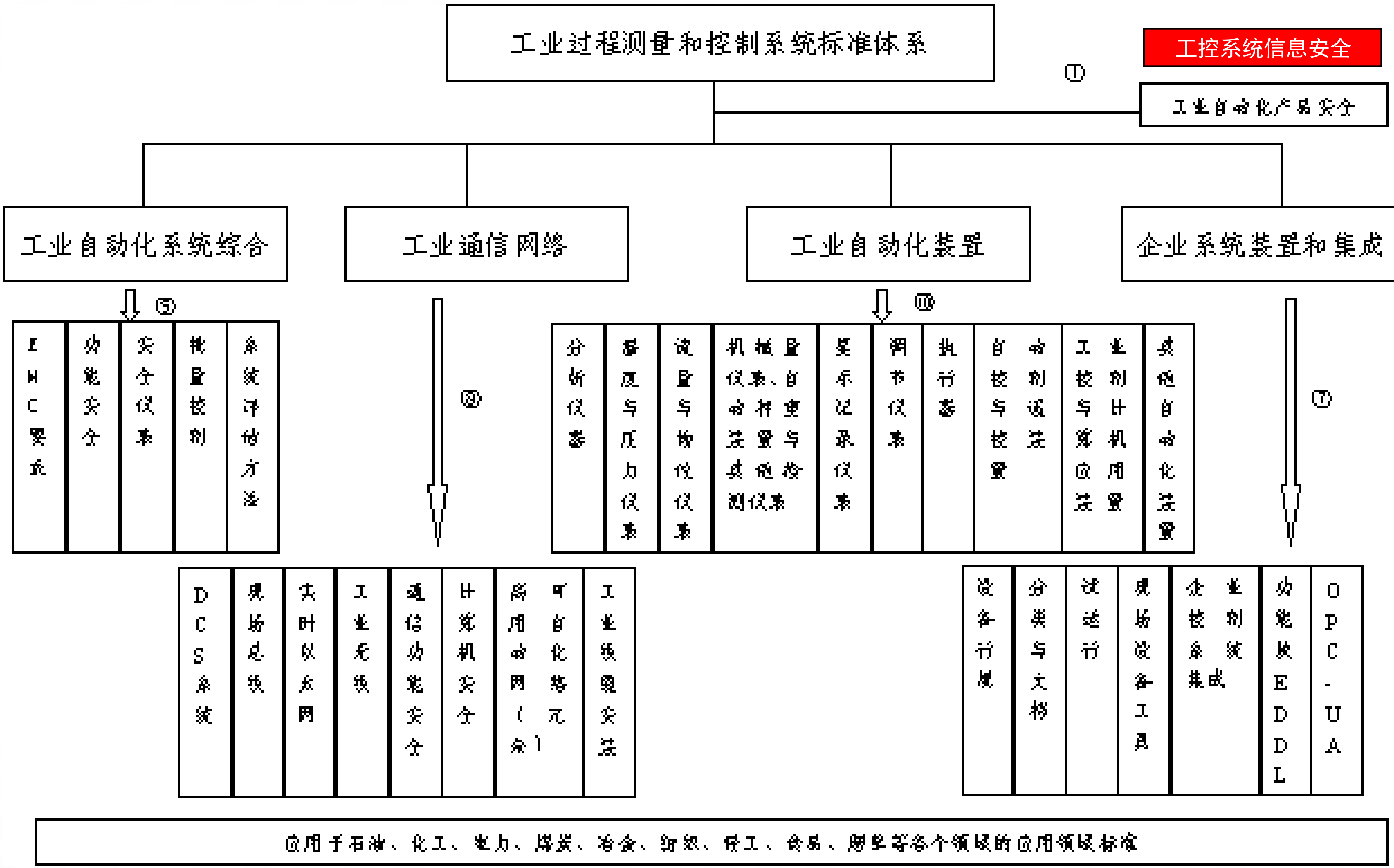
IEC 61508: 通用电气控制系统
IEC 62061: 机械电气控制系统
IEC 61511: 过程电气控制系统
IEC 61131-6: 功能安全PLC

- **工业信息安全**

IEC 62443（制定中）

IEC/TC65邀请中国专家梅恪(ITEI)参加IECEE W2B(工业自动化工作组)

我国的标准工作组


工业过程测量和控制系统标准体系
工控系统信息安全
工业自动化产品安全
工业自动化系统综合
工业通信网络
工业自动化装置
企业系统装置和集成
EMC要求
功能安全
安全仪表
批量控制
系统评估方法
DCS系统
现场总线
实时以太网
工业无线
通信功能安全
计算机安全
工业线缆安装
分析仪器
温度与压力仪表
流量与物位仪表
机械量仪表、自动衡器装置与无损检测仪表
显示记录仪表
调节仪表
执行器
工业控制与计算机应用装置
其他自动化装置
设备行规
分类与文档
试运行
现场设备工具
企业控制系统集成
功能块EDDL
OPC-UA
应用于石油、化工、电力、煤炭、冶金、纺织、轻工、食品、制药等各个领域的应用领域标准

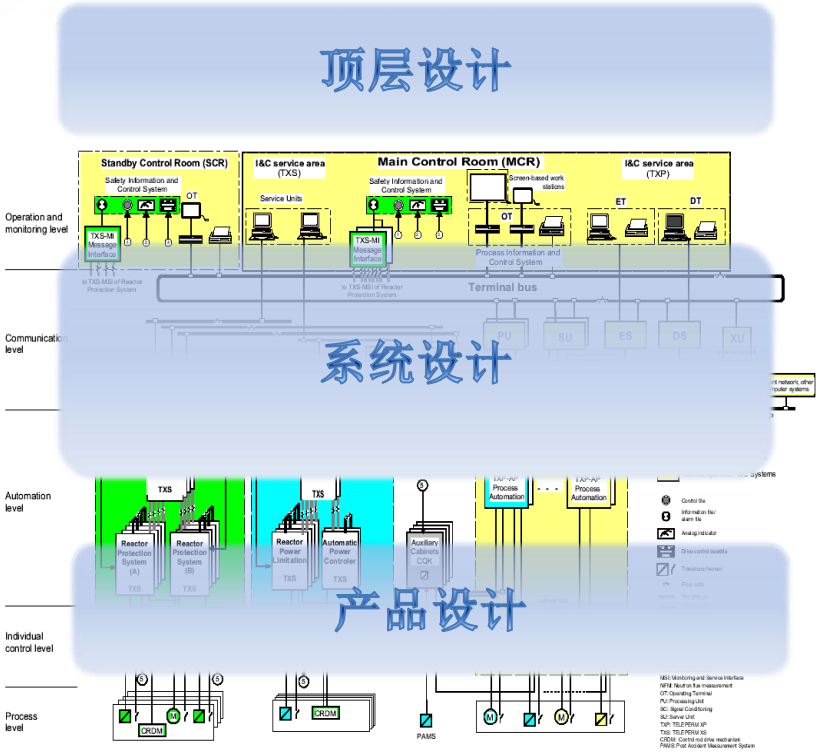
信息安全标准体系

■ 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；

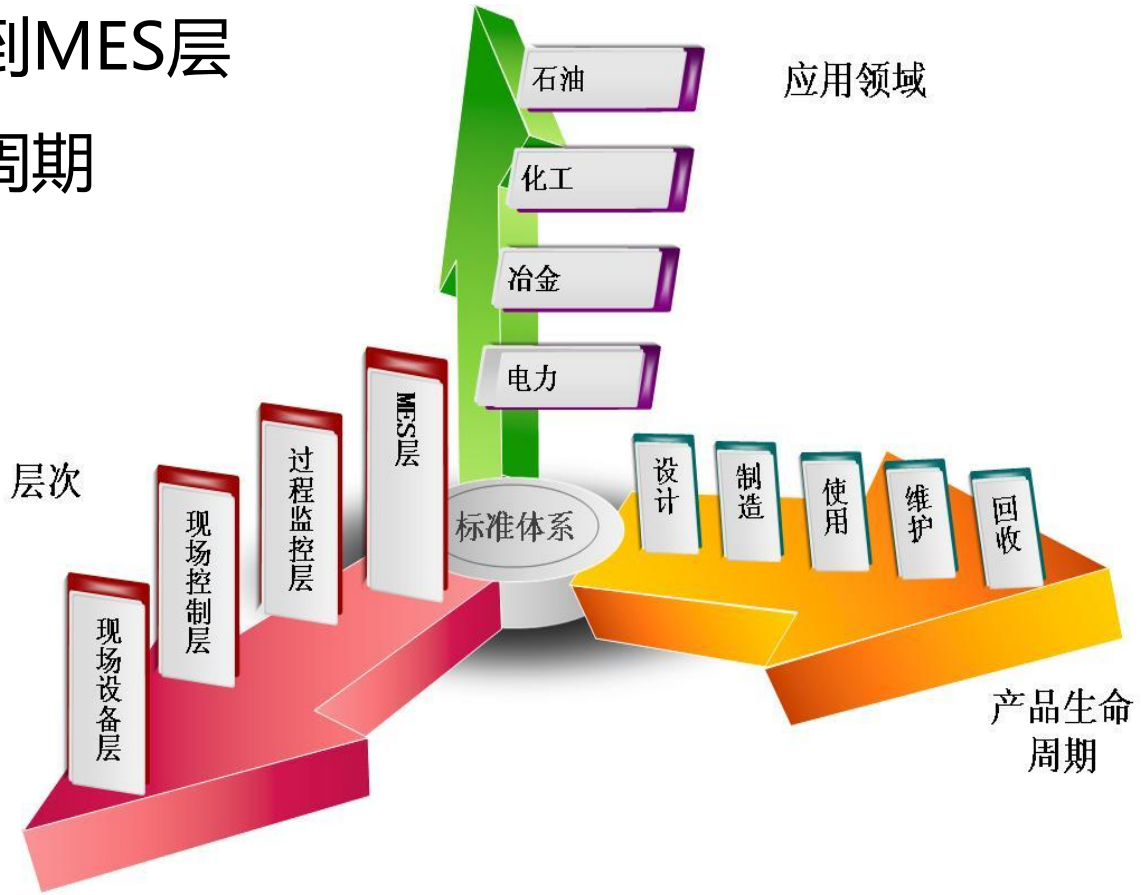
» 系统设计：建立了DCS、现场总线、PLC系统安全设计规范；

» 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

- 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

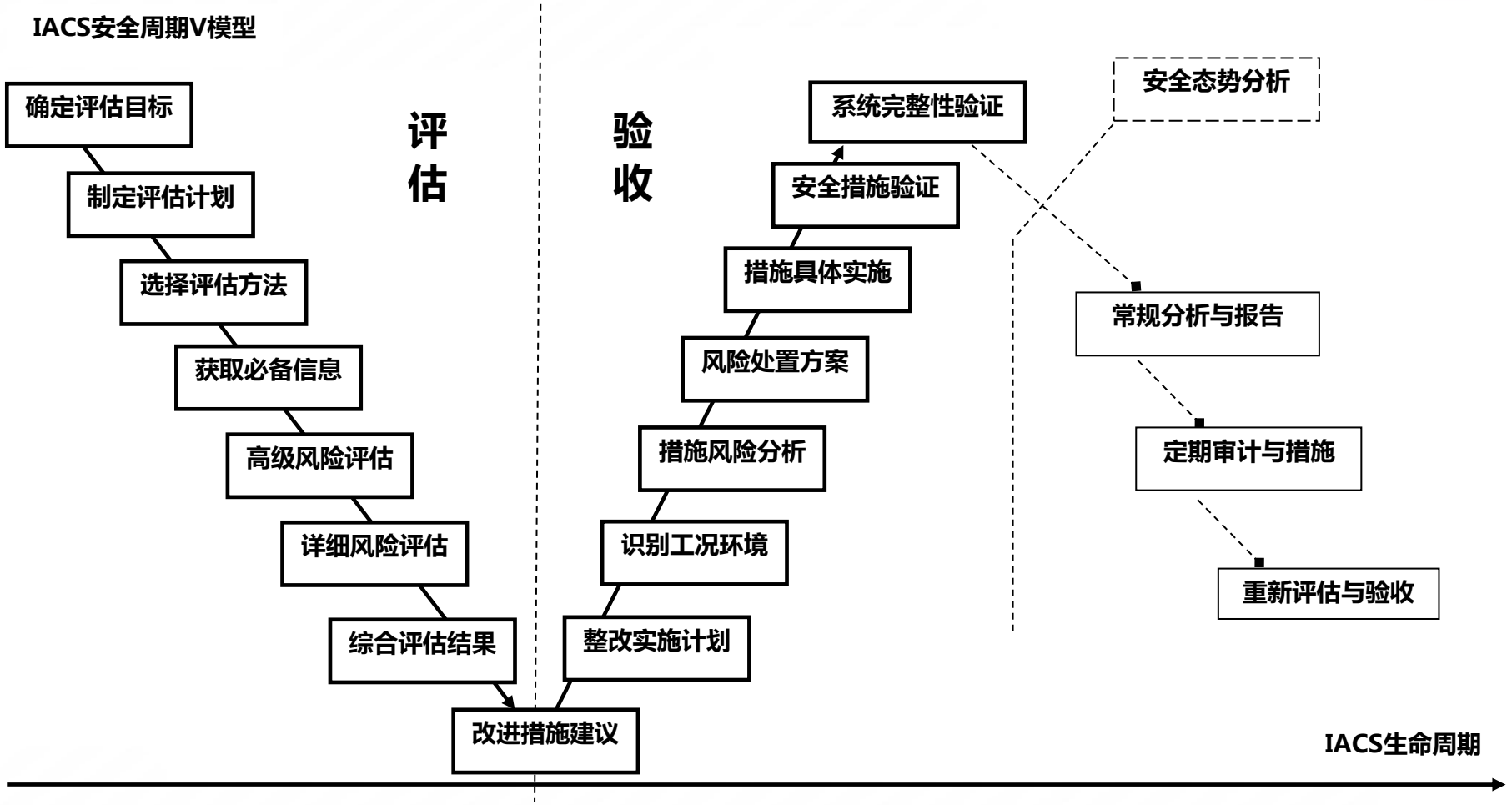
已发布国家标准（2项）	国家标准计划项目（6项）	已发布行业标准（3项）
• GB/T 30976.1-2014 工控系统信息安全 第1部分：评估规范 • GB/T 30976.2-2014 工控系统信息安全 第2部分：验收规范	• 20120829-T-604 工业通信网络 网络和系统安全 第2-1部分（ 等同 IEC 62443-2-1：2010）（10月送审） • 20130783-T-604 集散控制系统（DCS）安全防护标准（10月送审） • 20130784-T-604 集散控制系统（DCS）安全管理标准（10月送审） • 20130785-T-604 集散控制系统（DCS）安全评估标准（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

- 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

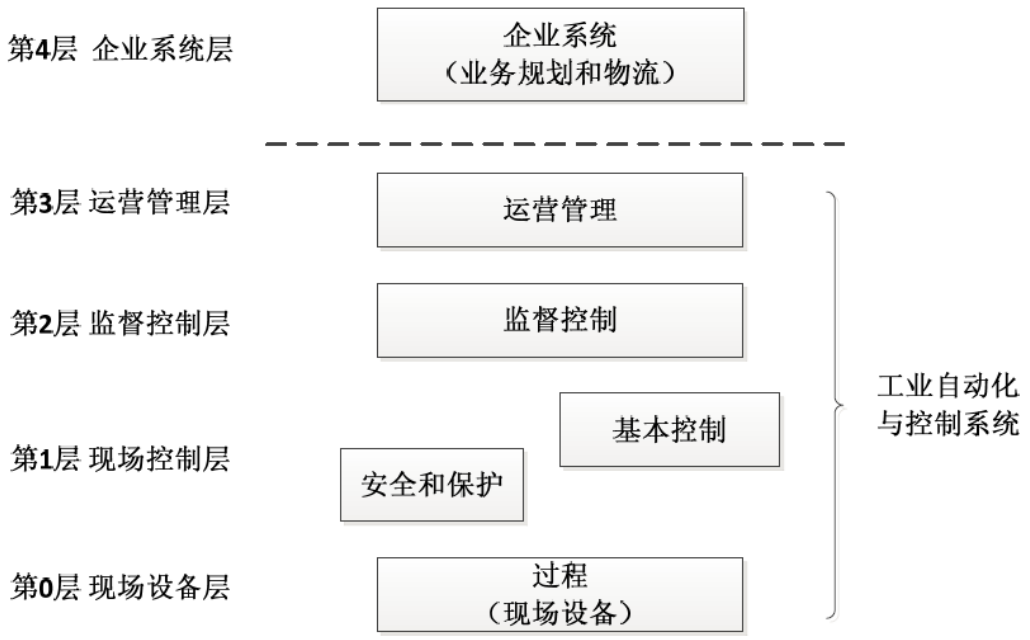


PLC系统信息安全要求

» 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

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

- 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

（德意志银行的金库不可能让美国上锁！）

致 谢!