工业信息安全标准体系建设与实践

2017

甘俊杰

2017.11.08

中国电子技术标准化研究院
China Electronics Standardization Institute

目 录
CONTENTS

1 政策形势

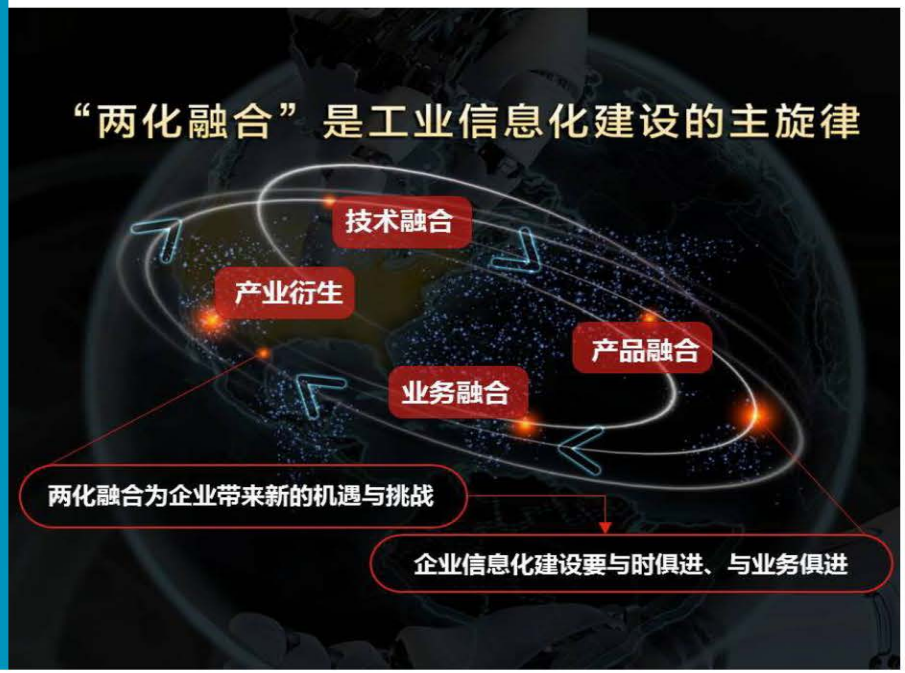
政策法规

- 为切实做好工业信息安全保障工作，主管部门发布系列政策文件和法规：
  - 《关于加强工业控制系统信息安全管理的通知》（工信部协〔2011〕 451号）
  - 《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》（国发〔2012〕23号）
  - 《关于开展2015年智能制造试点示范专项行动的通知》 （工信部装〔2015〕 72号）
  - 《国务院关于深化制造业与互联网融合发展的指导意见》（国发〔2016〕28号）
  - 《关于加强国家网络安全标准化工作的若干意见》（中网办发文〔2016〕5号）
  - **《中华人民共和国网络安全法》（2016.11）**
  - **《工业控制系统信息安全防护指南》（工信部信软〔2016〕338号）**

- 2016年5月26日，在第20届中国国际软件博览会上，苗部长指出：“要提高工业信息系统安全水平。制定实施工业控制系统信息安全防护指南，完善标准体系。”

- 从国内外形势和产业发展看出，工业信息安全防护工作极端重要。
- 标准作为政策规划落实的重要抓手，为工业信息安全防护工作提供重要支撑。

2 政策形势
两化融合



我国的两化深度融合正处于战略机遇期、发展攻坚期，未来将以两化融合为主线协同推进两个强国建设。一方面，智能制造是两化深度融合的主攻方向，加快推动互联网等新一代信息技术与传统制造业融合发展，成为加快制造强国建设的关键抓手；另一方面，制造业是发展数字经济的主战场，随着互联网应用领域从消费环节向制造环节的渗透扩散，网络空间范围不断扩展，推进两化融合为网络强国建设提供重要支撑。

3 政策形势
互联网+

互联网突破了地域、组织、技术的界限，推动制造业创新主体高效互动、产品快速迭代、模式深刻变革、用户深度参与，制造业中创客空间、创新工场等新载体、新模式不断涌现，激发全社会创新活力、提高创新资源配置效率、缩短技术商业化周期，推动制造业从要素驱动型发展向创新驱动型升级。可见，制造业的壮大需要利用互联网等新技术，互联网发展也需要以制造业为主战场。

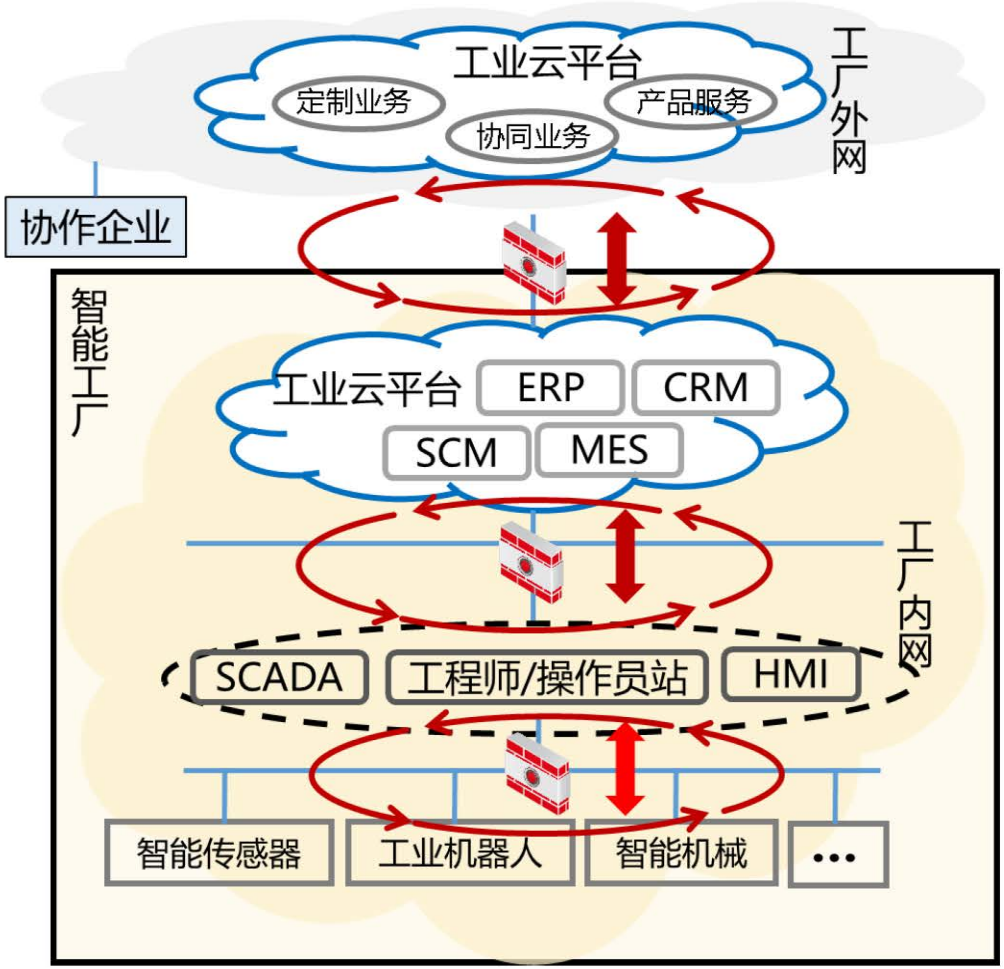
4 政策形势
工业安全

控制环境开放化使外部互联网威胁渗透到工厂控制环境

控制安全

网络IP化、无线化以及组网灵活化给工厂网络带来更大的安全风险

网络安全



数据的开放、流动和共享使数据和隐私保护面临前所未有的挑战

数据安全

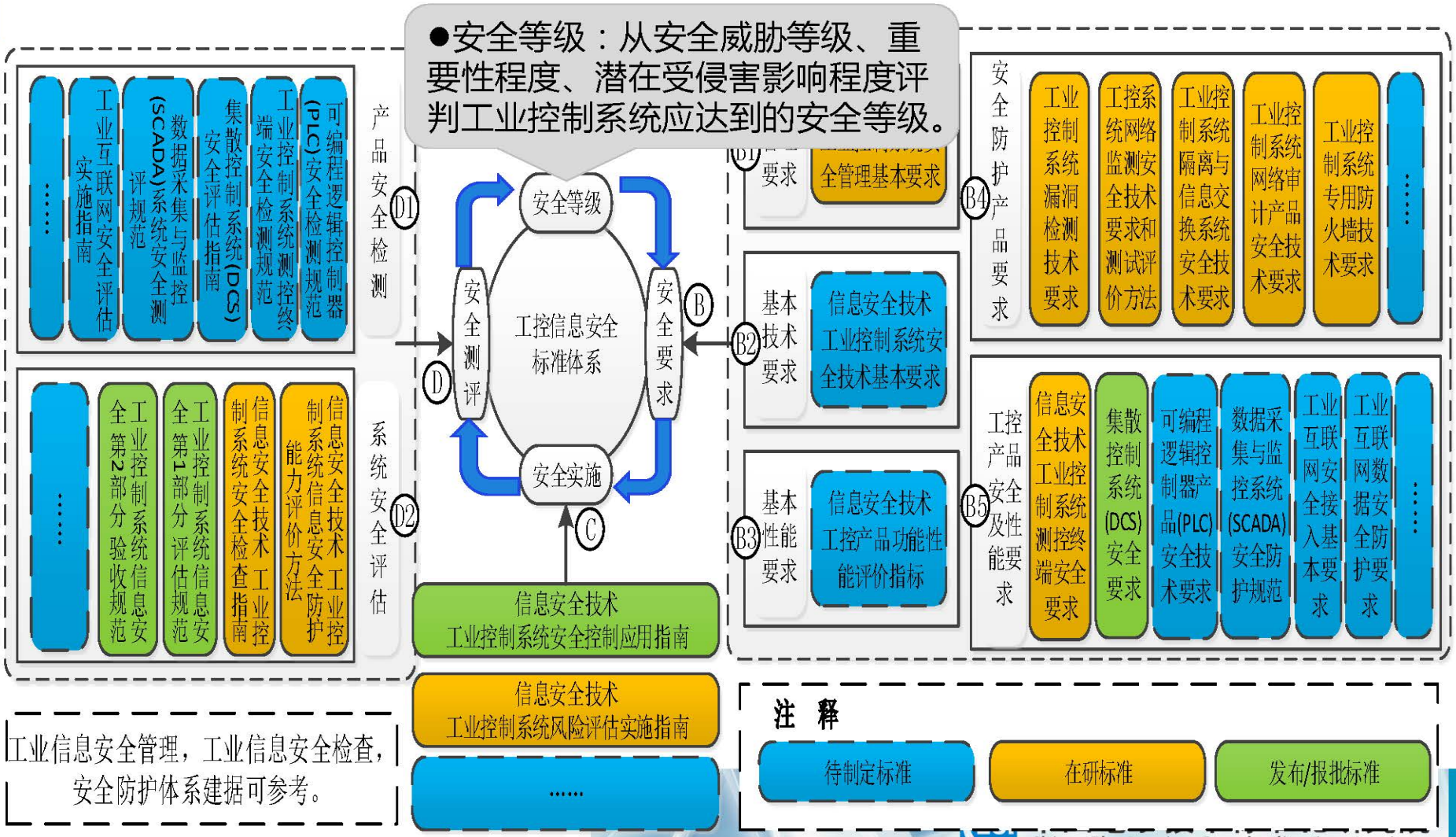
设备智能化使生产装备和产品暴露在网络攻击之下

设备安全

目 录
CONTENTS

1 标准体系

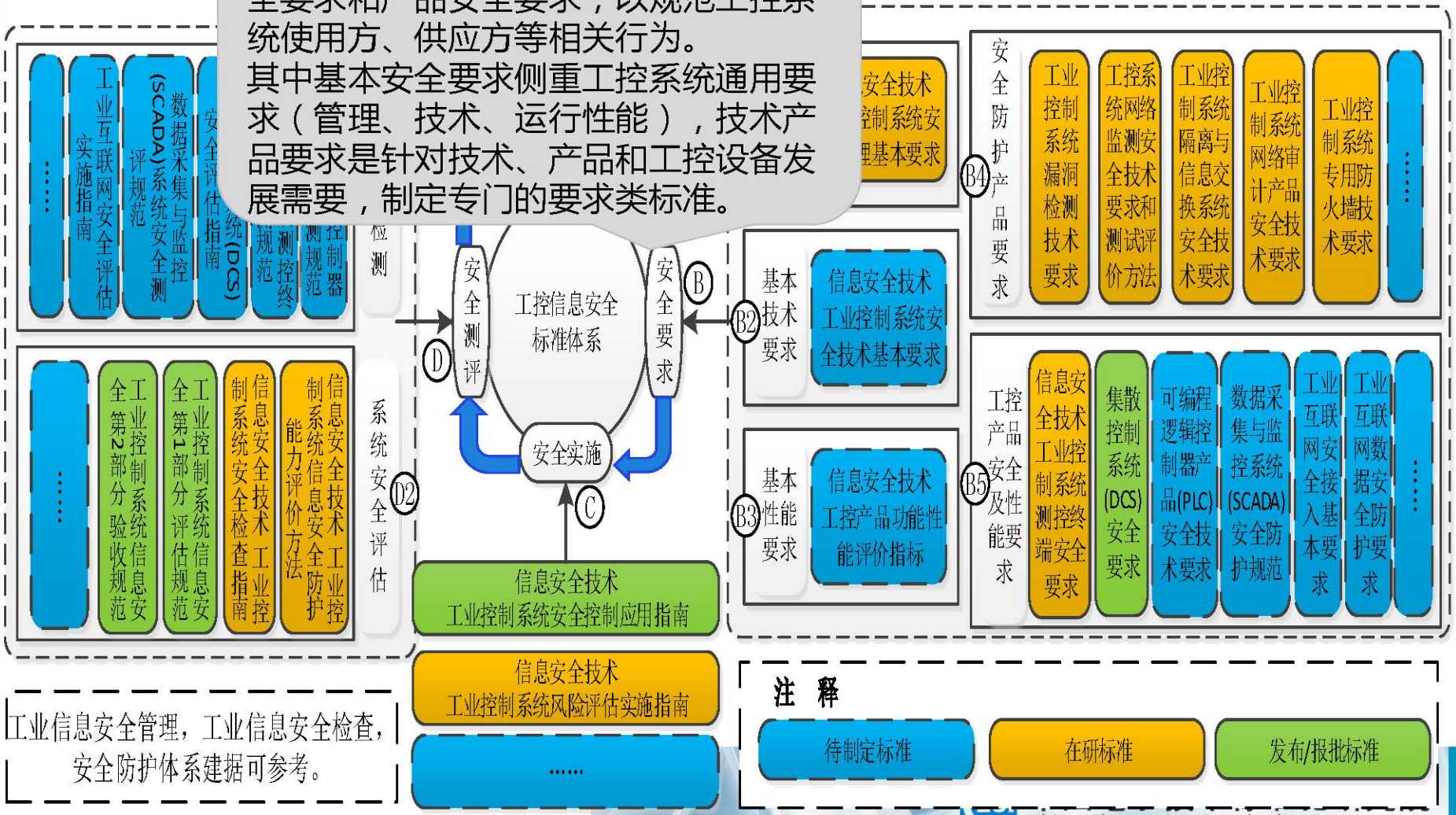
工控安全为核心



1 标准体系

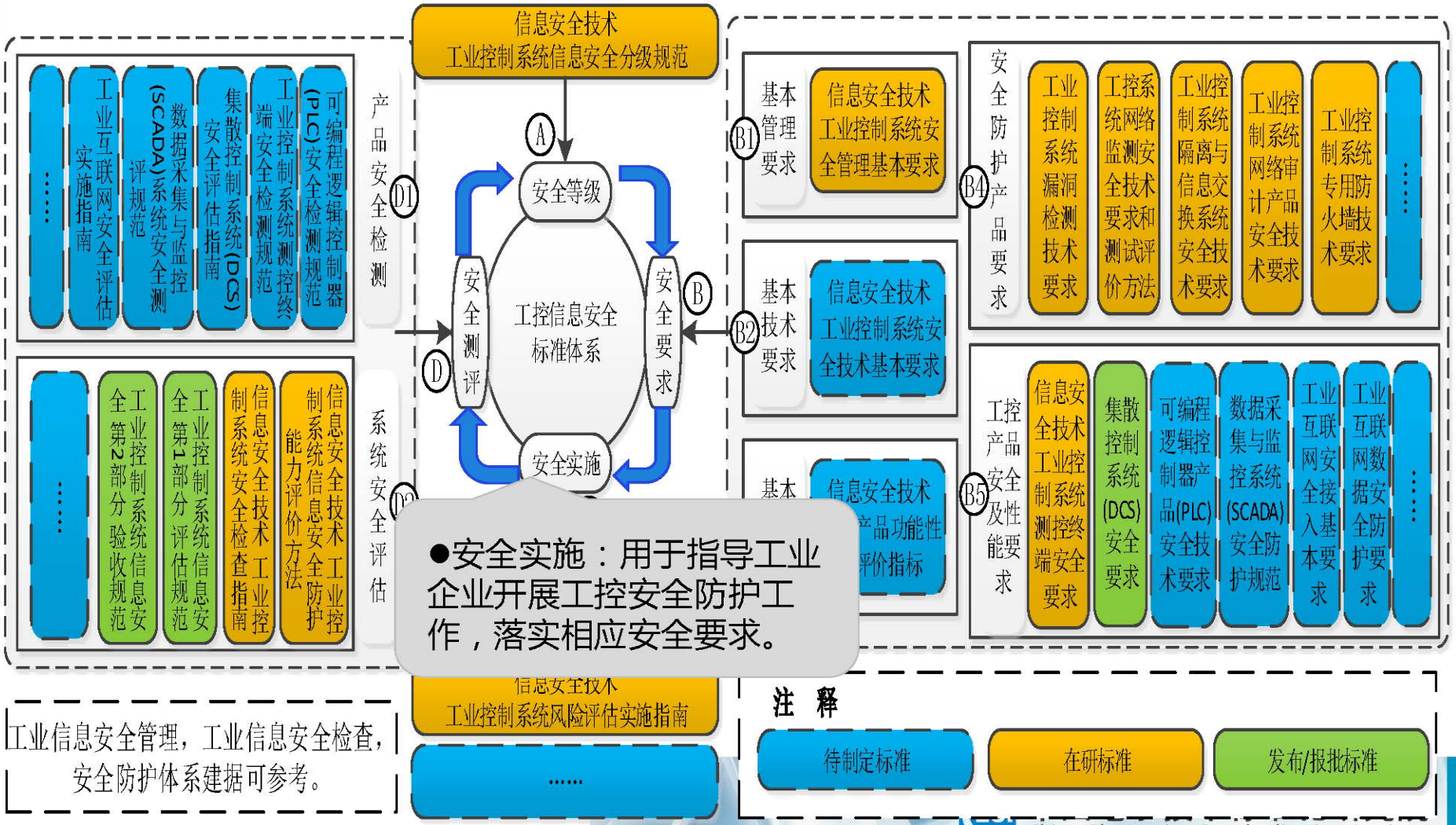
工控安全为核心

●安全要求：分为工业控制系统基本安全要求和产品安全要求，以规范工控系统使用方、供应方等相关行为。
其中基本安全要求侧重工控系统通用要求（管理、技术、运行性能），技术产品要求是针对技术、产品和工控设备发展需要，制定专门的要求类标准。

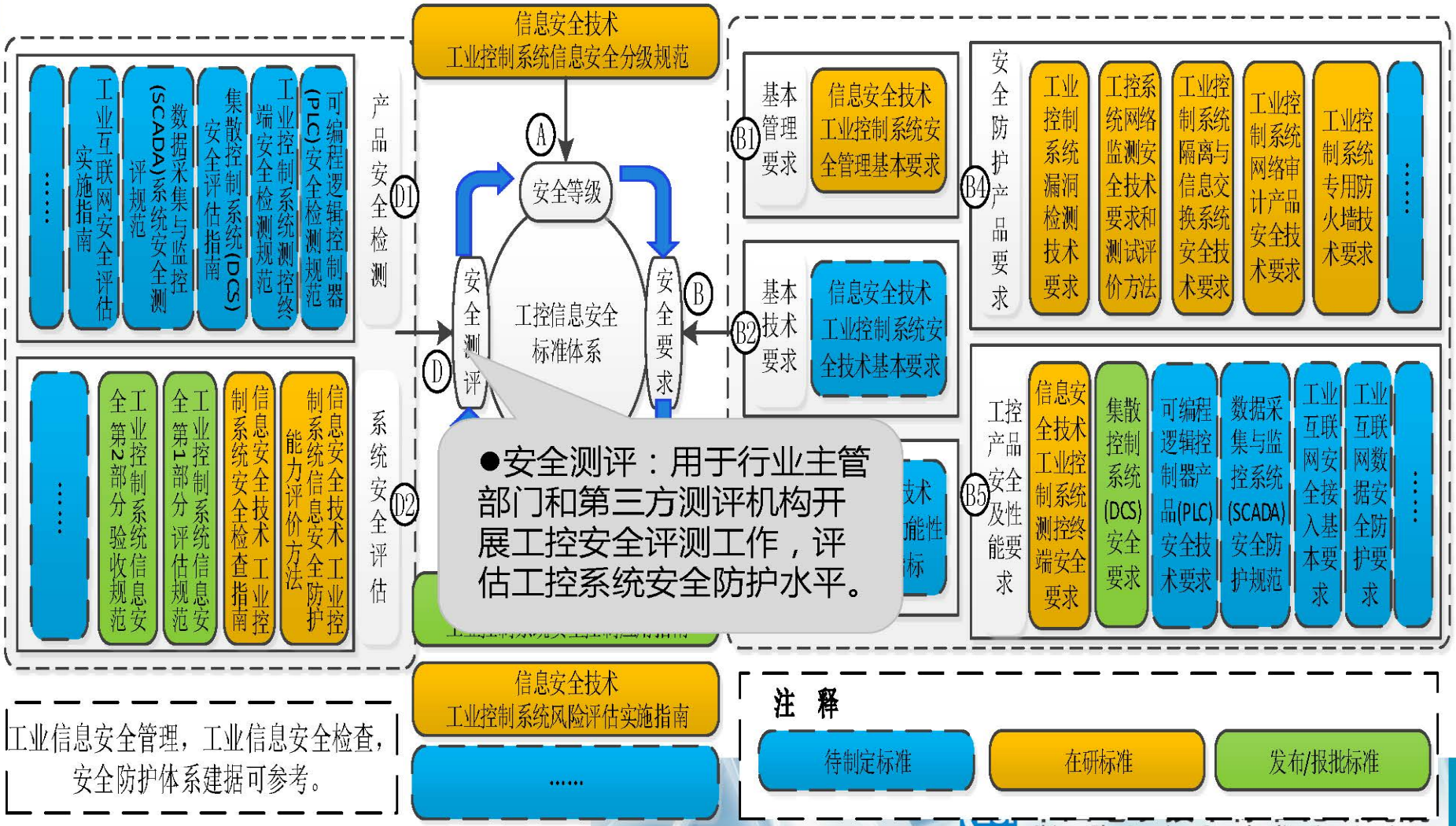


工业信息安全管理，工业信息安全检查，安全防护体系建据可参考。

1 标准体系
工控安全为核心



1 标准体系
工控安全为核心

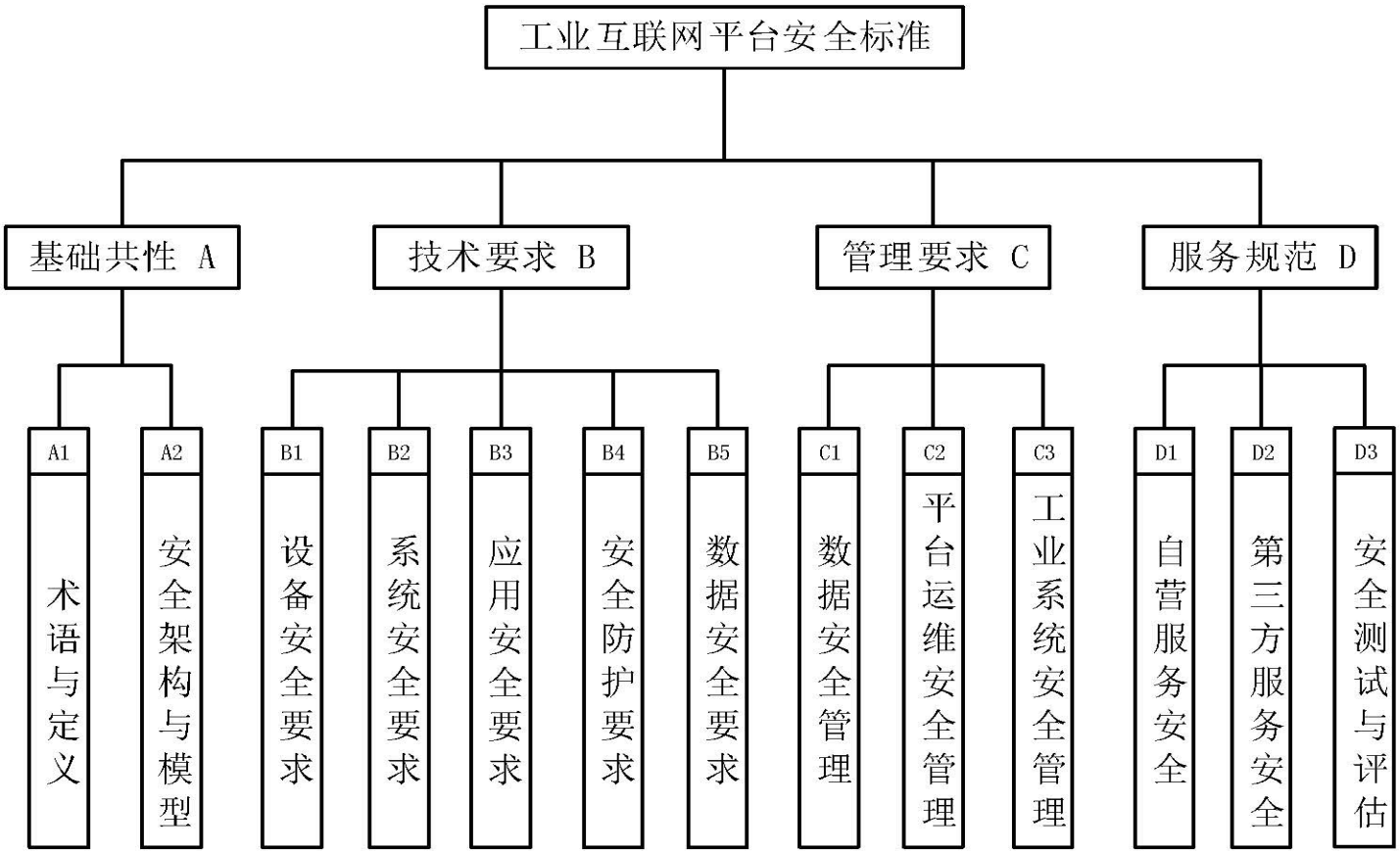


2 标准体系
工控安全标准国标概况

序号	标准名称	所出状态
1	《信息安全技术 工业控制系统安全控制应用指南》（GB/T 32919-2016）	发布
2	《信息安全技术 工业控制系统安全分级指南》	报批稿
3	《信息安全技术 工业控制系统安全管理基本要求》	报批稿
4	《信息安全技术 工业控制系统测控终端安全要求》	报批稿
5	《工业控制系统风险评估实施指南》	征求意见稿
6	《信息安全技术 工业控制系统安全检查指南》	征求意见稿
7	《信息安全技术 信息系统安全等级保护基本要求 第5部分：工业控制系统》	草案
8	《信息安全技术 工业控制系统安全防护技术要求和测试评价方法》	草案
9	《信息安全技术 工业控制系统网络审计产品安全技术要求》	征求意见稿
10	《工业控制系统专用防火墙技术要求》	征求意见稿
11	《信息安全技术 工业控制系统网络监测安全技术要求和测试评价方法》	征求意见稿
12	《信息安全技术 工业控制系统漏洞检测技术要求》	征求意见稿
13	《信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求》	征求意见稿
14	《工业控制系统产品信息安全评估准则 第1部分 简介和一般模型》	征求意见稿
15	《工业控制系统产品信息安全评估准则 第2部分 安全功能要求》	征求意见稿
16	《工业控制系统产品信息安全评估准则 第3部分 安全保障要求》	征求意见稿

3 标准体系

工业互联网平台标准体系



4 标准体系

工业互联网平台标准明细

总序号	分序号	标准名称
1	B1设备安全	工业互联网终端设备安全基本要求
2		工业互联网平台硬件安全技术要求
3	B2系统安全	工业互联网平台系统安全技术要求（包含系统、软件）
4	B3应用安全	工业互联网平台安全接入规范
5		工业互联网平台应用安全基本要求
6	B4安全防护	工业互联网安全防护基本要求
7		工业互联网安全防护产品技术要求
8		工业互联网平台网络安全监测技术要求
9	B5数据安全	工业互联网平台数据安全防护基本要求
10		工业互联网数据交换安全规范
11	C 安全管理	工业互联网平台数据生命周期安全管理要求
12		工业互联网平台安全运维管理规范
13	D 服务安全	工业互联网平台自营服务安全基本要求
14		工业互联网平台第三方交易服务安全规范
15		工业互联网平台安全评估实施指南
16		工业互联网平台安全防护产品测试评价指标

目 录
CONTENTS

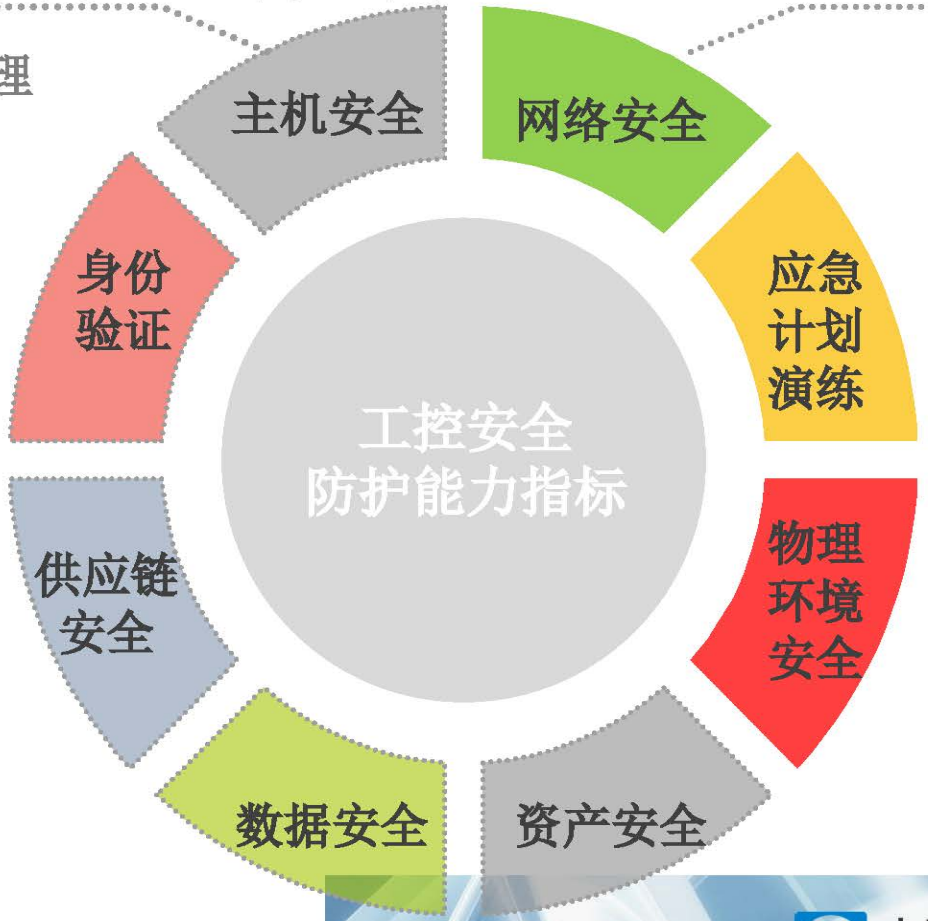
1 标准解读

工业控制系统信息安全防护能力评价方法

依据评价计划，针对如下指标，开展工业控制系统信息安全防护评价工作。
共11个大项，30个小项，129个安全问题。

✓安全软件选择与管理

✓配置和补丁管理



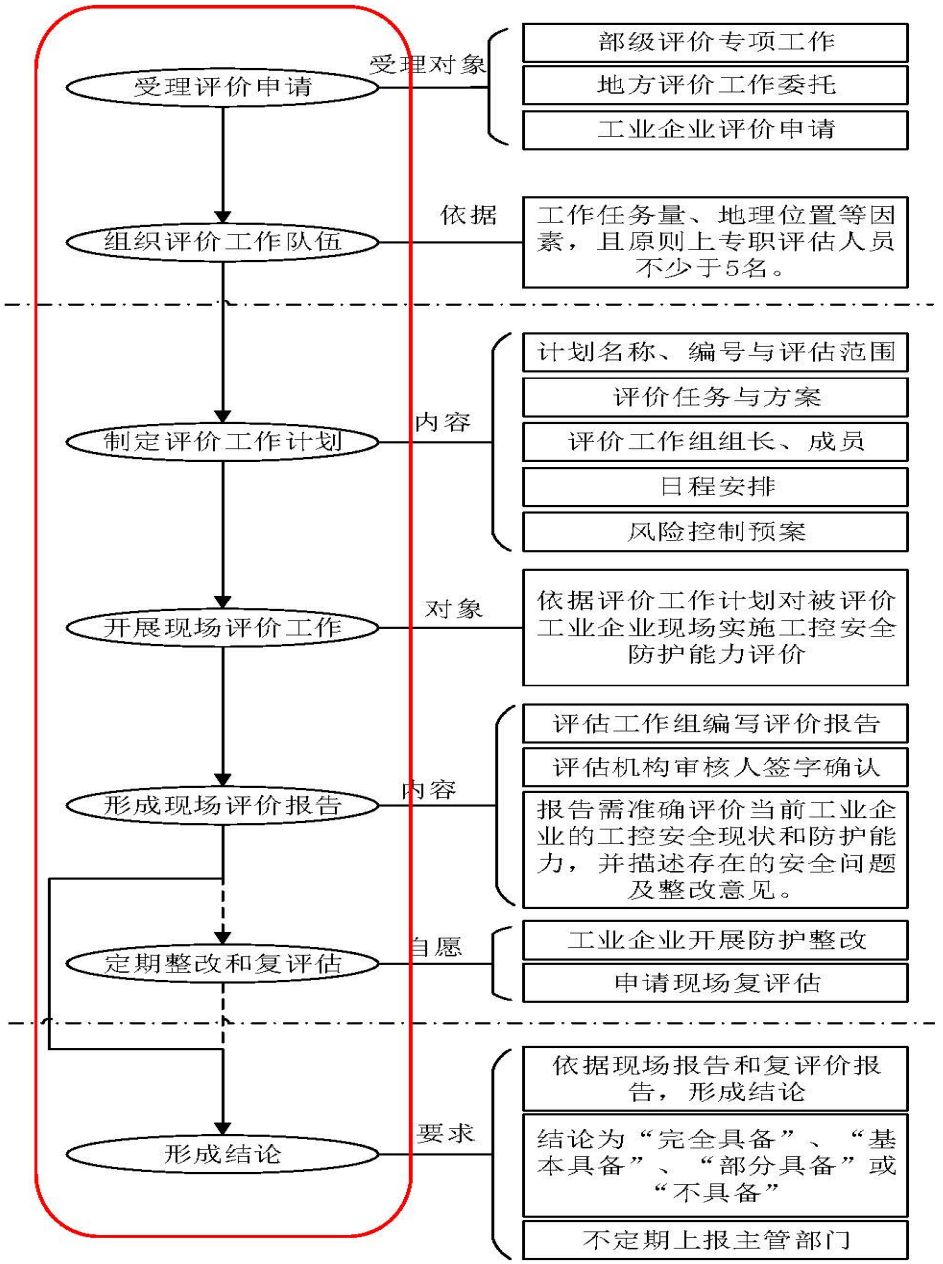
✓工控网络边界防护

✓远程访问安全

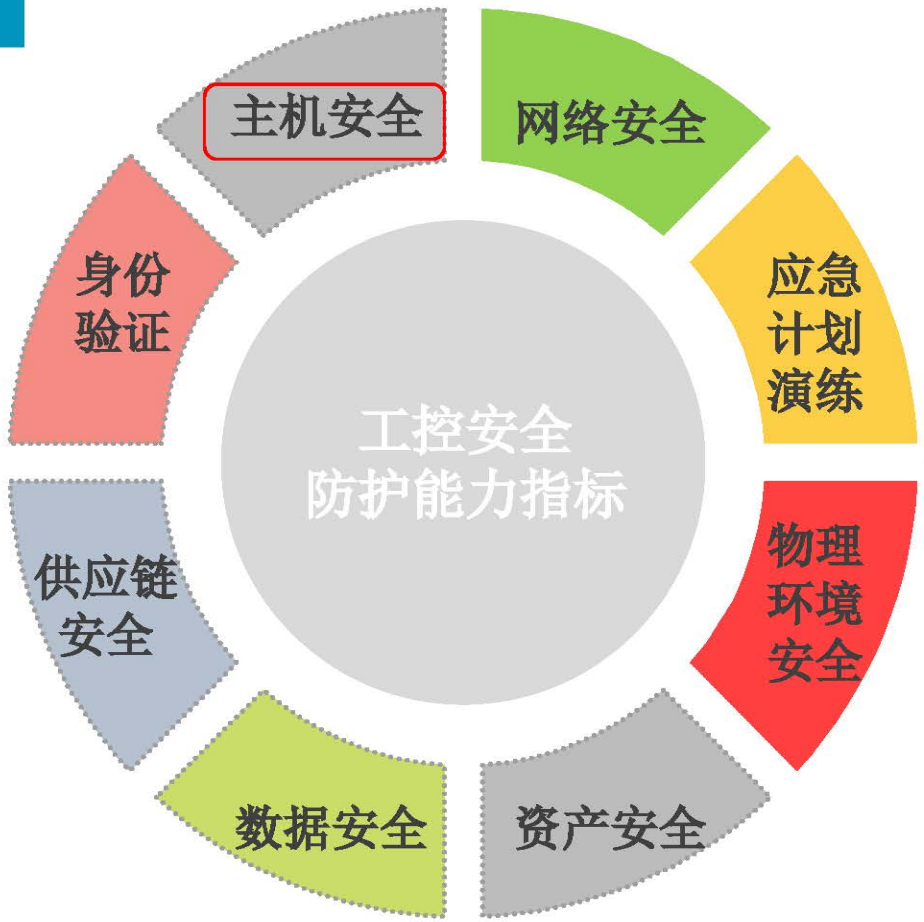
2 标准解读

防护能力评价方法

针对各行业工业控制系统安全防护工作的特点，提出了工业控制系统安全防护评价流程，从**工作流程**、**评价队伍组建**、**制定评价工作计划**、**安全防护能力评价指标**、**现场报告形成**、**整改复评**、**形成结论**等方面对工业控制系统安全防护评价工作提出了规范性指导，以满足不同组织对其工业控制系统的安全管理需求，为实现对工业控制系统适度、有效的安全管理控制提供参考。



3 标准解读
防护能力评价表



评分操作方法表

主项	要求	评价	分值
一、安全软件选择与管理（4项9分）	（一）在工业主机上采用经过离线环境中充分验证测试的防病毒软件或应用程序白名单软件，只允许经过工业企业自身授权和安全评估的软件运行	1.防病毒软件或应用程序白名单软件的来源不安全正规，扣X分； 2.工业主机未安装防病毒软件或应用程序白名单软件，扣X分；	5
		4.防病毒软件或应用程序白名单软件未在离线环境测试，扣X分。	3
	（二）建立防病毒和恶意软件入侵管理机制，对工业控制系统及临时接入的设备采取病毒查杀等安全预防措施	5.未建立防病毒和恶意软件管理制度，扣X分；（若本项不满足，略过第6-8项） 6.防病毒和恶意软件管理制度不完备、合理；扣X分；	4
		9.未定期对工业控制系统进行查杀，扣X分； 10.未对临时接入的设备进行查杀，扣X分。	2
二、配置和补丁管理（7项13.5分）	（一）做好工业控制网络、工业主机和工业控制设备的安全配置，建立工业控制系统配置清单，定期进行配置审计	11.未建立工业控制网络的安全配置策略，扣X分； 12.未建立工业主机的安全配置策略，扣X分； 13.未建立工业控制设备的安全配置策略，扣X分；	6

目 录
CONTENTS

1 建设实践
检查评估

2016年11月，中央网信办组织实施国家网络安全关键信息基础设施检查。
2017年4月，工信部信软司开展工业控制系统信息安全防护能力预评估工作。
2017年7月，工信部信软司组织工业控制系统信息安全检查。



2 建设实践
试点验证

2017年5月-9月，依据上述标准，组织工信部电子一所、软测、赛迪等单位，牵头带队赴国家电网、上汽集团、中一药业、华天科技等单位，开展标准试点评估工作，验证标准的科学有效性。

国网江苏省电力公司

上海汽车集团股份有限公司

广州白云山中药一业有限公司

甘肃天水华天科技股份有限公司

3 建设实践
共性问题

通过国家网络安全关键信息基础设施检查、工业控制系统信息安全防护能力预评估、工业控制系统信息安全检查工作，初步摸清了我国工业企业安全防护现状，也发现了一些共性问题。

4 建设实践
下一步工作

核心技术 + **标准化** + **软硬件** + **生态系统**

加强基础技术、通用技术、非对称技术、前沿技术、颠覆性技术的科研攻关和协同创新

加大自主创新工业互联网安全标准研制力度

开展国产芯片、操作系统、数据库、信息安全等关键软硬件应用试点示范

推动工业互联网安全新技术、新产业、新业态、新模式的孕育发展

中国电子技术标准化研究院
China Electronics Standardization Institute