中国智能制造2025中的功能安全

Functional Safety in Chinese Smart Manufacturing 2025

史学玲 教授

Prof. Shi Xueling

2019.9.24（德国）

机械工业仪器仪表综合技术经济研究所

Instrumentation Technology and Economy Institute (ITEI)

内容

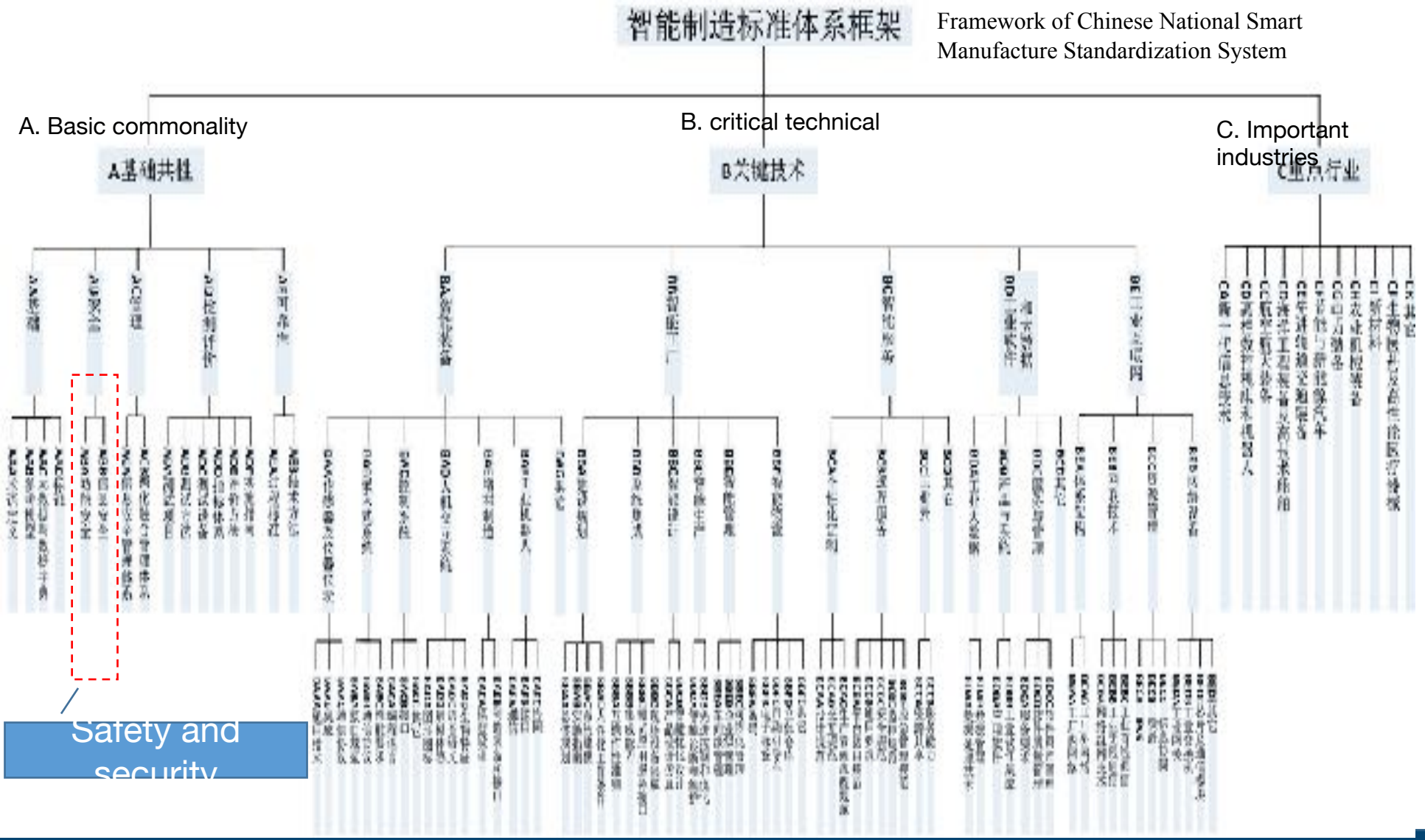
- ✓ 功能安全在中国智能制造框架体系中的位置
- ✓ The Position of Functional Safety in Chinese Smart Manufacturing Framework System
- ✓ 中国在功能安全方面的政策要求
- ✓ China's Policy Requirements on Functional Safety
- ✓ 中国在功能安全方面的标准要求
- ✓ China's Standard Requirements for Functional Safety

内容

- ✓ 正在做的标准
- ✓ Standards under preparation
- ✓ 正在研究实现的技术
- ✓ Technologies under Research and Implementation
- ✓ 正在研究解决的问题
- ✓ Problems under study
- ✓ 合作建议
- ✓ Cooperation proposal

功能安全在中国智能制造标准体系框架中位置

Functional Safety in the Framework of Chinese Smart Manufacturing Standard System



中国在功能安全方面的政策要求

China's Policy Requirements on Functional Safety

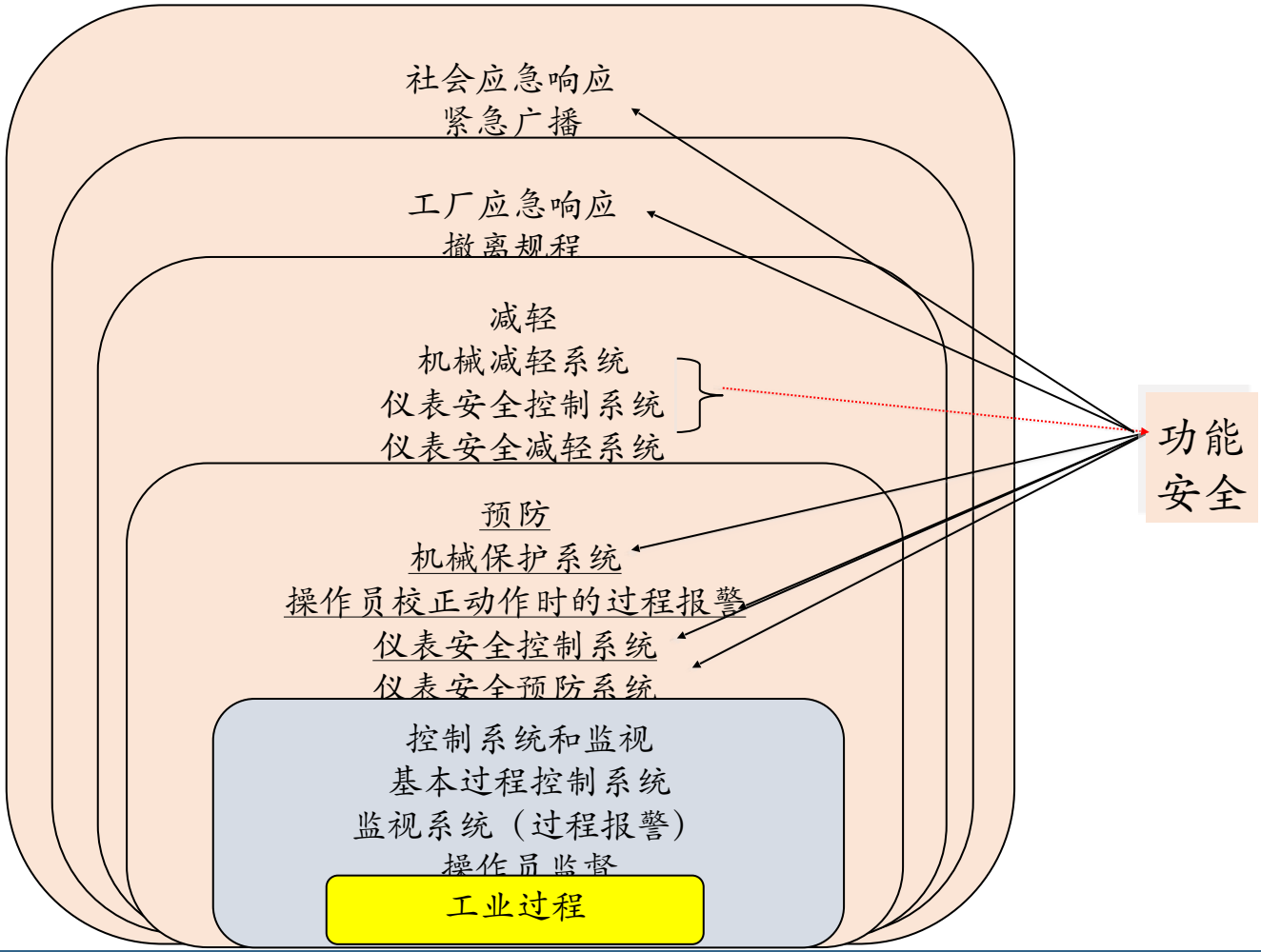
国家安全监管总局关于加强化工过程安全管理的指导意见
Guidance Opinions of the State Administration of Safety Supervision on Strengthening Safety Management in Processing
安监总管三〔2013〕88号 （2013年7月29日）

提出了过程安全管理要求
Requirements for process safety management are put forward.

国家安全监管总局关于加强化工安全仪表系统管理的指导意见
Guidance of the State Administration of Safety Supervision on Strengthening the Management of Industrial Safety Instrument System
安监总管三〔2014〕116号 （2014年11月13日）

提出了功能安全的管理要求
The management requirements of functional safety are put forward.

目前安全仪表系统功能安全的要求已经成为高危企业获得生产许可证的条件之一At present, the requirement of functional safety of safety instrument system has become one of the conditions for high-risk enterprises to obtain production license



中国在功能安全方面的标准要求
China's Standard Requirements for Functional Safety

GB/T 20438.1~7《电气/电子/可编程电子安全相关系统的功能安全》，等同采用IEC61508
GB/T 20438.1-7 "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems", equivalent to IEC 61508

GB/T 21109.1~3《过程工业领域安全仪表系统的功能安全》，等同采用IEC61511
GB/T 21109.1~3 "Functional Safety of Safety Instrument System in Process Industry", equivalent to IEC 61511

GB/T 35320-2017《危险与可操作性分析（HAZOP）应用指南》
GB/T 35320-2017 Guidelines for the Application of Hazard and Operability Analysis (HAZOP)

GB/T 32857-2016《保护层分析（LOPA）应用指南》，等同采用IEC61882

GB/T 32857-2016 Guidelines for the Application of Protection Layer Analysis (LOPA), equivalent to IEC 61882

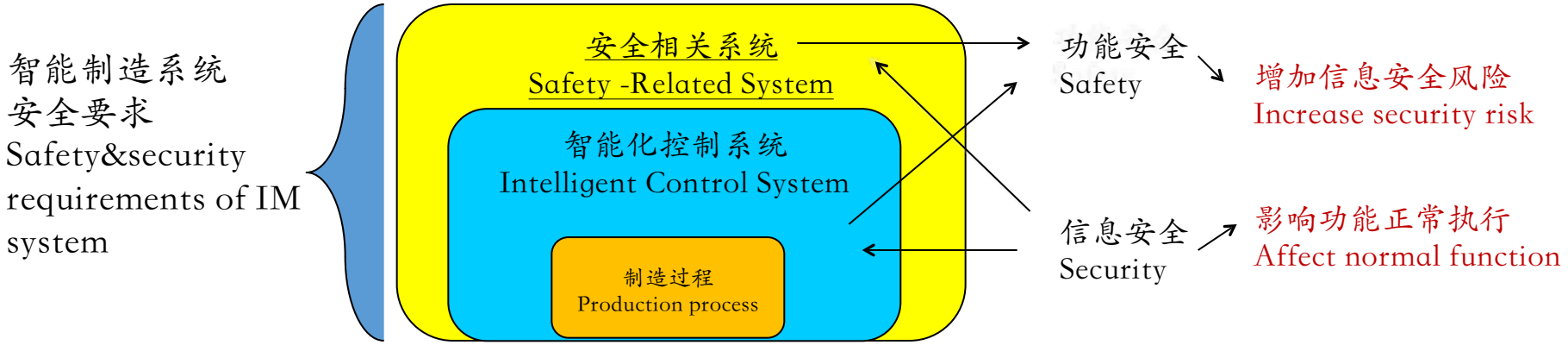
中国在功能安全方面的标准要求
China's Standard Requirements for Functional Safety

GB/T 32202-2015《油气管道安全仪表系统的功能安全 评估规范》
GB/T 32202-2015 Standard for Functional Safety Assessment of Oil and Gas Pipeline Safety Instrument System

GB/T 32203-2015《油气管道安全仪表系统的功能安全 验收规范》
GB/T 32203-2015 Standard for Functional Safety Acceptance of Safety Instrument System for Oil and Gas Pipeline

关于风险减轻系统的功能安全标准正在讨论制订中
Functional safety standards for risk mitigation systems are under discussion

我们在智能制造系统功能安全的考虑
Consideration of Functional Safety in Intelligent Manufacturing Systems



- ✓ 安全走多远，技术才能走多远
- ✓ How far can safety go, then how far can technology go
- ✓ 目的：保证智能化系统功能正确，并在实现互联互通、信息集成的同时，系统正确执行设计的功能
- ✓ Objective: To ensure the function of smartsystem is correct, and to implement the designed function correctly while realizing interconnection and information integration.
- ✓ 免于制造系统功能失效导致的不可接受风险，提出制造系统的功能安全
- ✓ Avoid the unacceptable risk caused by the failure of manufacturing system function, and put forward the functional safety of manufacturing system.
- ✓ 免于智能化系统功能失效导致的不可接受风险，提出智能化系统的功能安全
- ✓ Avoid the unacceptable risk caused by the function failure of intelligent system, and put forward the function safety of intelligent system.
- ✓ 保证高可靠性的同时，实现故障管理，避免失效
- ✓ Ensuring high reliability, at the same time, achieving fault management and avoid failure

正在制订的国家标准
National Standards under preparation

- 智能工厂 安全监测有效性评估规范
- Standard for Evaluating the Effectiveness of Safety Monitoring in Intelligent Factory
- 智能工厂 安全控制要求
- Safety Control Requirements of Intelligent Factory
- 数字化车间功能安全要求
- Functional Safety Requirements of Digital Workshop
- 数字化车间信息安全要求
- Cyber Security Requirements of Digital Workshop
- 数字化车间可靠性要求
- Reliability Requirements of Digital Workshop
- 数字化车间/智能工厂安全一体化要求
- Safety Integration Requirements of Digital Workshop/Intelligent Factory

旨在规范智能制造升级改造过程中的安全实现—智能制造的安全保障

The aim is to standardize the safety realization in the process of upgrading and transformation of intelligent manufacturing-the safety guarantee of intelligent manufacturing

智能安全 Intelligent safety

- 法律法规自符合 Laws and regulations are self conforming
- 环境自适应 Environmental adaptation
- 动态安全距离 Dynamic safety distance
- 人员能力分级 Classification of personnel ability
- 设备能力分级 Equipment capability classification
- 工作职责分配到每天和每个人 Assign responsibilities to everyone and every day
- 识别并控制了所有风险 Identify and control all risks
- 动态的风险评估与控制 Dynamic risk assessment and control

正在研究解决的问题
Problems under study

问题 Problem :

a) 智能化之后系统更加复杂，暴露出更多的风险和漏洞，更容易受到外部攻击。功能安全设计必须同时考虑信息安全风险和漏洞的防护。必须考虑功能安全和信息安全的相互作用和潜在的副作用。

a) systems are more complexity, more vulnerability and more like to be attacked. The mutual impact between safety and security may be good or bad.

正在研究解决的问题
Problems under study

问题Problem :

b) 为实时的响应客户的要求，生产系统程序的变更更加频繁并需要及时响应。系统漏洞的检测及修复要求，使得设备固件升级的要求变得更加频繁。

- 在线升级接口（工具）的设计约束；
- 变更的检测和报警接口的要求，及其对资产管理软件设计的要求；
- 实时检测恶意更改和恢复的要求；

b) To achieve customization production quickly, modification of production systems software become more frequently. Online detection for fault and vulnerability require firmware updating more frequently. All above generate:

- new requirements for online update interfaces or tools;
- new requirements for online detection and alarm interface, including asset management tool
- protection of malicious changes and restore

正在研究解决的问题
Problems under study

问题Problem：

c) IIoT工业物联网 Industry Internet of Things

d)工业云的应用限制？例如：云MES平台？ Limited to Industry cloud? Cloud platform MES?

e) 无线的应用限制？ Limited to Wireless?

f) 安全操作HMI？ New safety and security requirements for HMI? Emergency stop button?

g) 安全和非安全混合系统？Integration of safety and NON-safety systems, the interface between safety and non-safety is more and more blur.

h)应急管理要求带来的安全和安保的接口？ safety and security management? For example the interface for safety and security emergency information.

j)智能工厂或数字化车间环境内产生新的危险源 Intelligent factory or digital workshop environment generates new risk sources

正在研究解决的问题
Problems under study

问题Problem：

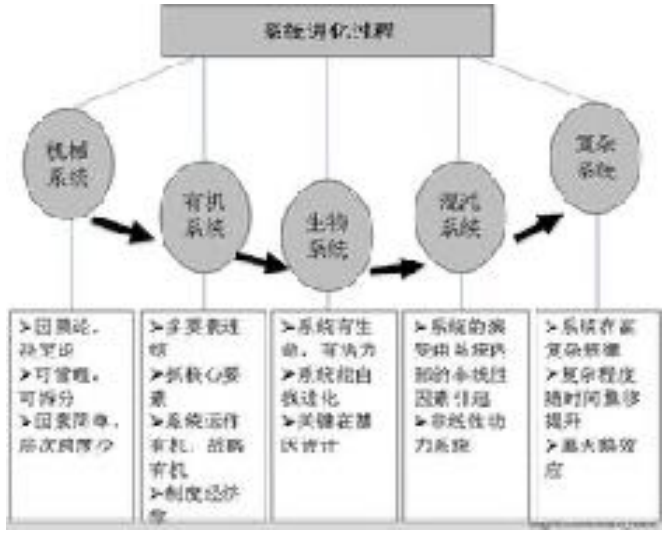
k) 控制逻辑复杂化导致功能错误危险 The complexity of control logic leads to functional error risk.

l)智能化技术和产品不成熟引入的安全问题 Safety problems are caused by immature intelligent technologies and products.

m)复杂系统运行的可信性问题 The credibility problem of complex system operation

n)公共服务支撑体系不成熟风险 Immature risk of public service support system

……



合作建议

Cooperation proposal

- 以中德标准化合作功能安全工作小组为核心，成立一个由中德双方专家参加的功能安全研究小组;
- With the Sino-German Standardization Cooperation Functional Safety Working Group as the core, a functional safety research group with experts from both sides was established.

- 每年在中国与德国举行研讨、交流、参观活动，共同研究技术，解决问题
- Every year, seminars, exchanges and visits are held between China and Germany to jointly study technology and solve problems.

- 工作组可逐步研究相关内容，分步实现最

研究目标：智能制造安全

Research objective:
Safety of Smart manufacturing

- 工作组可逐步研究相关内容，分步实现最终目标。
- The working group can gradually study the relevant content and achieve the ultimate goal step by step.

研究目标：智能制造安全
Research objective:
Safety of Smart manufacturing

谢谢Thank you

史学玲

Shi Xueling

机械工业仪器仪表综合技术经济研究所

Instrumentation Technology and Economy Institute (ITEI)

sxl@instrnet.com

Tel：18611724397