



工业控制系统
信息安全产业联盟
Industrial Control Systems Information Security Alliance

智能制造安全一体化

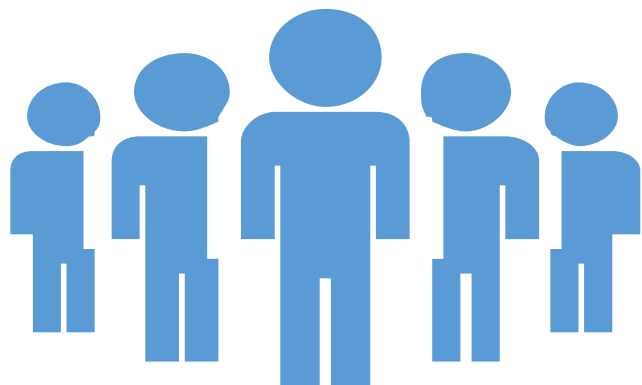
汇报人：机械工业仪器仪表综合技术经济研究所，孟邹清
汇报日期：2019年9月18日

目录

1	安全的本质
2	智能化时代的安全问题
3	一体化安全解决之道
4	思考与展望



01 安全的本质



安全的本质是 “没有不可接受的风险”

风险是某个事件或行为的不确定结果，这些事件或行为有可能影响人类的价值

01 安全的本质





02 智能化时代的安全问题

智能化时代的来临不可阻挡，安全问题如影随形

(机器人安全事故)

- 2015年6月29日，德国汽车制造商大众位于保纳塔尔的工厂发生意外，一名22岁的工人被机器人抓住，挤向了一块金属板，不幸身亡。
- 美国职业安全与健康管理局的统计数据显示，在美国，每年大约有一人死于与机器人有关的故事。





02 智能化时代的安全问题

智能化时代的来临不可阻挡，安全问题如影随形

(网络信息安全事件)

- 2010年，震网（Stuxnet）病毒曾感染了全球超过45000个网络，伊朗遭到的攻击最为严重，60%的个人电脑感染了这种病毒。
- 2011年，黑客通过入侵数据采集与监控系统SCADA，使得美国伊利诺伊州城市供水系统的供水泵遭到破坏。
- 2016年，三一重工近千台工程机械设备遭非法解锁破坏，数量多达近千台，波及多个省份，直接经济损失达3000余万元，间接损失近十亿元。
- 2018年，WannaCry的变种侵入了全球最大的代工芯片制造商台湾积体电路制造，导致其停产三天，预计经济损失高达17.4亿元人民币。
- 2019年，美国通过网络远程发起对委内瑞拉电网的攻击，造成电网瘫痪，引起公众对政府的不满，进而引发针对马杜罗政府的大规模游行示威活动。





02 智能化时代的安全问题

智能化时代的来临不可阻挡，安全问题如影随形

(人工智能安全事故)



Uber自动驾驶事故



特斯拉自动驾驶事故



IBM医疗保健漏洞



工业控制系统
信息安全产业联盟

机械工业仪器仪表综合技术经济研究所



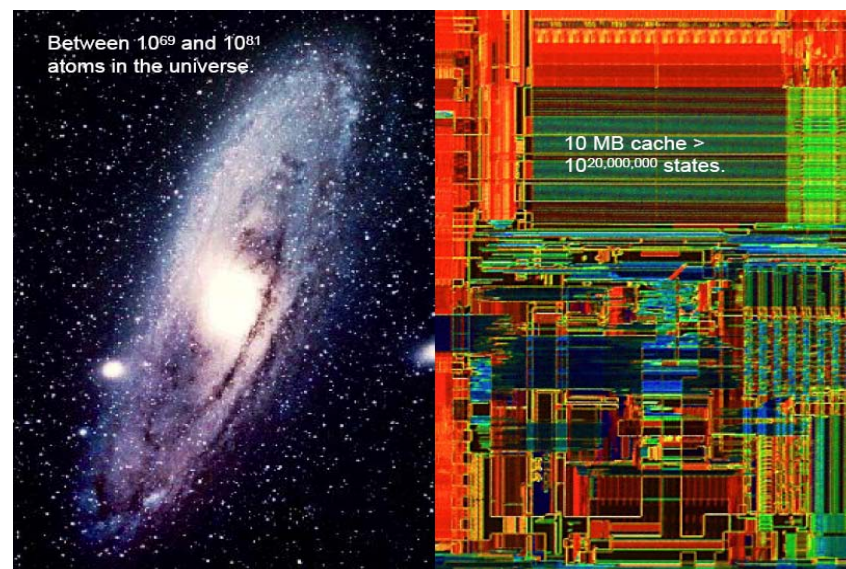
02 智能化时代的安全问题

安全问题的本源，是新技术发展应用的风险

(技术复杂性)

技术越来越复杂，采用大量电子、可编程电子元件、各类软件

- (1) 电子/可编程电子的安全设计理念还在不断研究之中；
- (2) 故障难以预计、发现和检测，失效现象不再直观可视；





02 智能化时代的安全问题

安全问题的本源，是新技术发展应用的风险

(技术不成熟)

人工智能
弱人工智能和强人工智能

机器学习
实现人工智能的一种方法

Machine Learning

深度学习
实现机器学习的一种技术

□ 技术缺陷

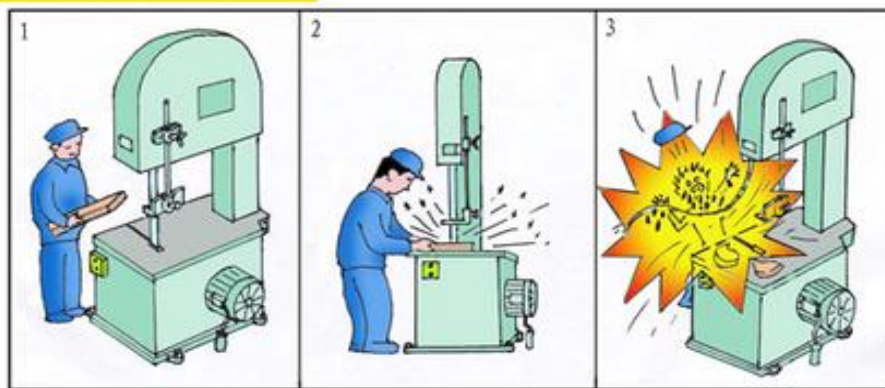
- 机器学习算法鲁棒性差;
- 数据集自身存在缺陷;
- 环境变化导致模型感知能力减弱;



安全问题的本源，是新技术发展应用的风险

(应用复杂性)

事故案例图解 (机械伤害)

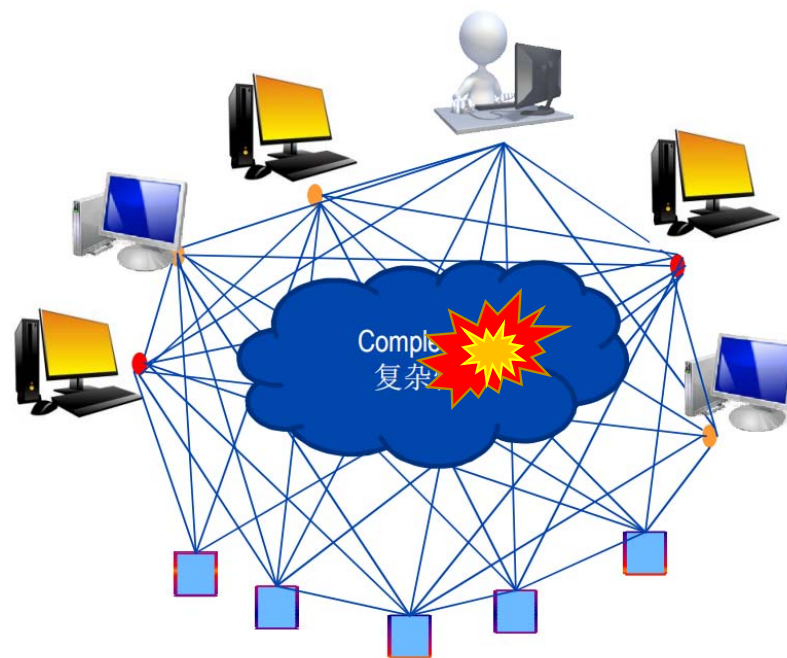


传统工业：

关注有限范围内的单体设备风险

网络化、智能化工业：

单元风险、连接风险、数据风险、应用风险...





02 智能化时代的安全问题

安全问题的本源，是新技术发展应用的风险

(体系不健全)



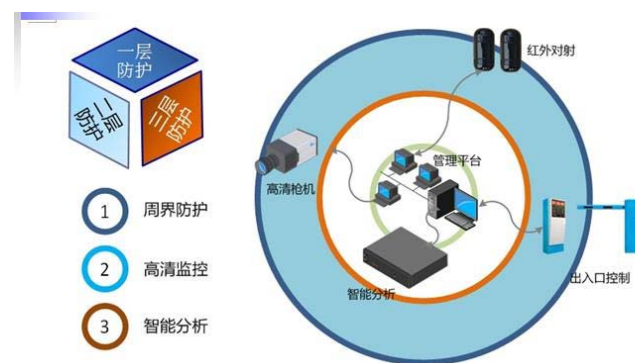


02 智能化时代的安全问题

智能化时代安全问题——如何解决

智能化的安全？

解决思路：采用安全一体化的方式，实现
网络化智能化工业应用的综合安全保障





03 一体化安全解决之道

智能化工业安全层级特征

层级	现场层	控制层	执行层	经营层
对象类型	设备、人员、基础设施	控制系统、网络（控制网、数采网、感知网、监视网）、应用、数据、人员	应用、信息网（内网）、数据、人员	应用、信息网（外网）、数据、平台、人员
智能化特征	智能装备、信息基础设施、伺服驱动器、智能IO、智能传感器、仪表、智能产品...	先进控制、实时优化	企业生产管理柔性化、智能任务分解和下达、生产动态分析和实时修正	综合利用数据仓库、联机处理、数据挖掘技术等新兴信息技术，协调企业各局部的生产过程，达到企业总体最优
安全特征	芯片、嵌入式操作系统、编码规范、第三方应用软件等： 可能存在漏洞、缺陷、规范使用、后门等安全挑战； 人员误操作	机床数控系统、PLC、运动控制器、控制协议、控制平台、控制软件等方面： 可能存在设计之初未考虑完整性、身份校验等安全需求； 输入验证，许可、授权与访问控制不严格，不当身份验证，配置维护不足，凭证管理不严，加密算法过时； 网络威胁、边界模糊等 人员误操作	应用平台和软件： 病毒、木马、漏洞等传统安全威胁； 复杂系统环境下，其功能、性能、安全是否合理、完整、可靠 人的社会工程学、钓鱼攻击、邮件扫描攻击等导致信息泄露的安全管理问题；	应用平台和软件： 病毒、木马、漏洞等传统安全威胁； 复杂系统环境下，其功能、性能、安全是否合理、完整、可靠； 人的社会工程学、钓鱼攻击、邮件扫描攻击等导致信息泄露的安全管理问题；



03 一体化安全解决之道

智能化工业安全风险分析

1、内部风险

构成智能工厂的单元由于自身的故障或缺陷导致安全事故的风险
(人、机、料、法、环)

2、外部风险

由于智能工厂外部的威胁、攻击等导致安全事故的风险

3、关联风险

智能工厂的单元由于上下游设备、相关过程、交互对象等的关联影响而失效，导致安全事故的风险

4、融合风险

自动化与信息化融合、互联网与生产操作网融合、功能安全保护与信息安全防护融合等的过程中引发冲突，导致安全事故的风险

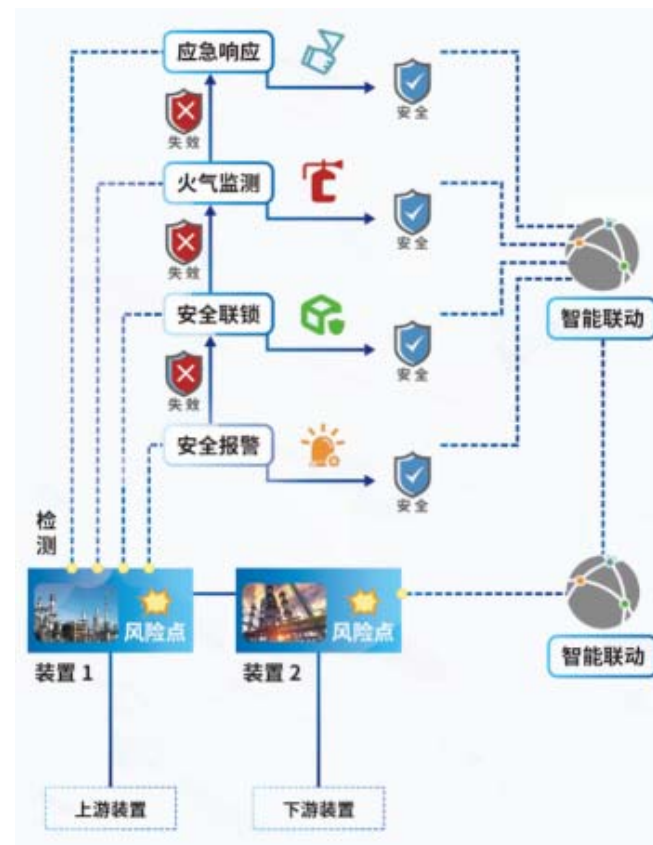


03 一体化安全解决之道

开放互联环境下的功能安全

报警、连锁、火气监测等功能安全系统层层作用保护生产安全。

各系统不再只是被动的触发，而是具备基于信息互联的分析预判主动防御能力，其可靠的工作以保持风险在合理可接受水平。





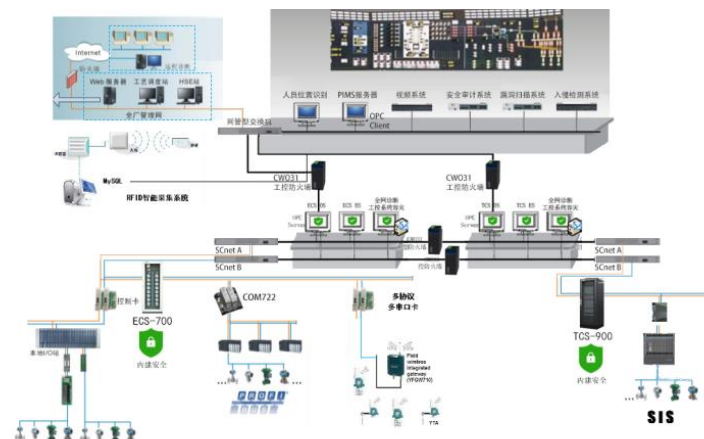
03 一体化安全解决之道

工业场景下的网络安全

网络攻击日趋多样化、复杂化，工业系统越来越处于开放的网络环境中。

传统IT信息安全技术手段远不能满足高危复杂多变的工业生产应用需求。

构建**纵深防御**、**内建安全**、**安全管理**和**应急响应**为一体的综合整体防护体系，提高工业系统安全性的同时，维持工业生产安稳运行。



工业控制系统
信息安全产业联盟
Industrial Control Systems Information Security Industry Alliance

机械工业仪器仪表综合技术经济研究所



03 一体化安全解决之道

功能安全和网络信息安全一体化协同防控

- 系统防护
System protection
- 信息安防
Information security
- 数据安防
Data security



功能失控

Function out of control

影响业务连续性

Influence business continuity

数据和信息泄密

Data and information leakage



功能安全

Functional Safety

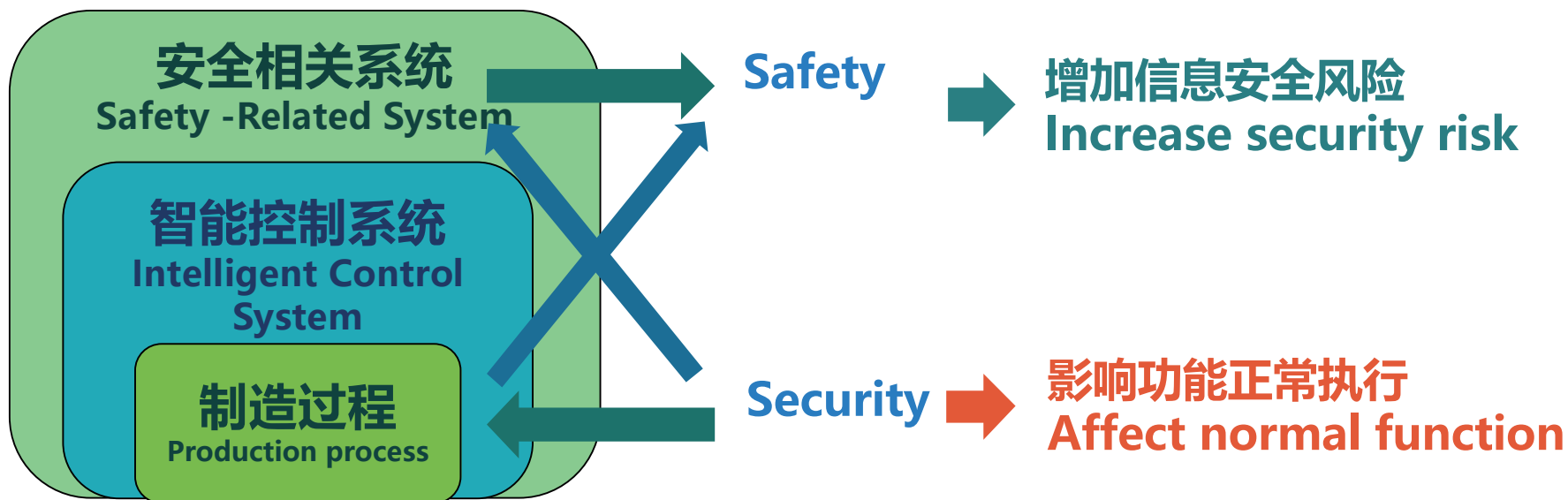
主要目标： 避免失控！
Avoid lose Control

安全一体化，安全集成化



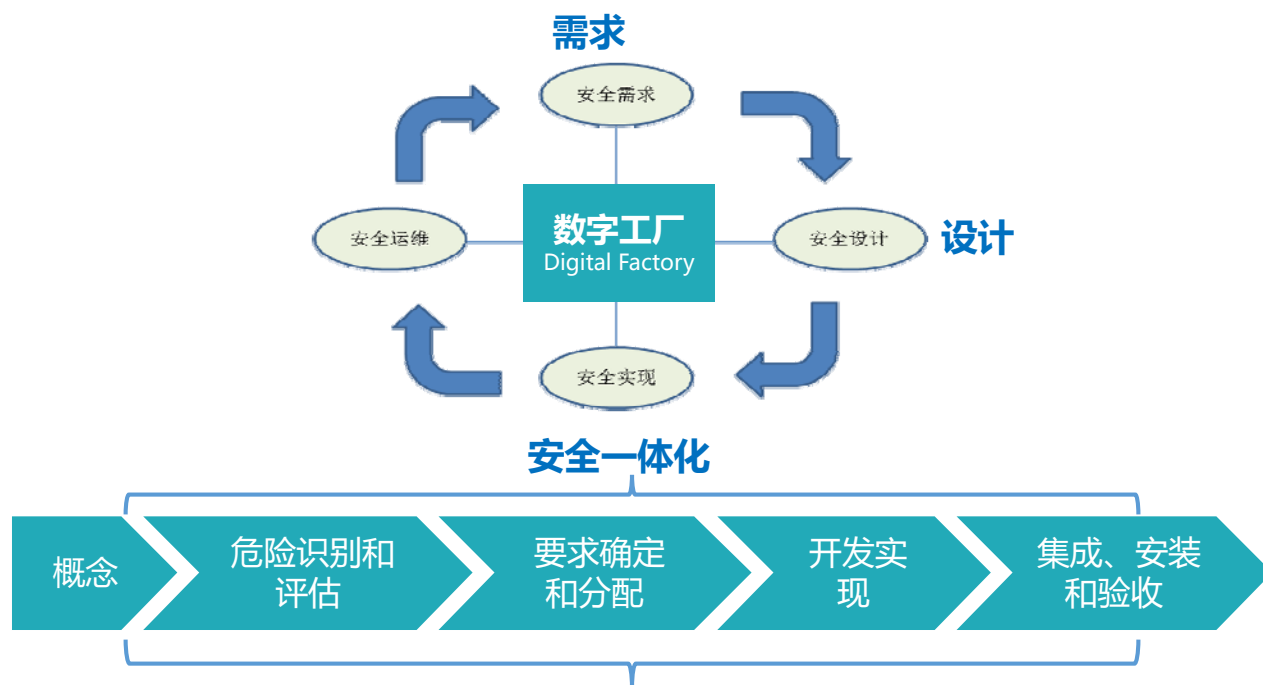
03 一体化安全解决之道

功能安全和网络信息安全一体化协同防控



功能安全系统、工业网络安全设施等各类安全技术措施协同作用，既共同实现对内安全控制和对
外安全防护，又不会因彼此间存在冲突而导致生产安全风险事件发生

安全一体化生命周期



需求分析阶段：定义Safety 功能、Security功能、安全完整性等级、安全防护能力、安全完善度等级等安全一体化目标；

设计、实施、运行、维护、变更、退役等各个阶段采取管控措施以保证目标得以实现和维持



03 一体化安全解决之道

安全一体化保障体系



证明安全的技术

- 审核
- 评估
- 验证
- 确认

综合标准化和实验验证体系

组成安全的技术

- 智能设备
- 子系统
- 系统产业链

产业提升和技术进步

(IEC61882, IEC61508 (GB/T20438), IEC61511 (GB/T21109), GT/T30976)



04 思考和展望

技术层面

- 工业化和网络化融合安全属于新兴领域，典型风险场景、融合安全技术指标、融合界面、融合风险和保障技术需要进一步研究和发掘；
- 应尽快研究建立风险原则和评判标准；在新兴技术领域，要做到安全风险可接受准则和评价标准的科学、实用，技术上可行，应用上可操作，尚需要时间
- 人工智能、大数据等在安全保障领域的应用是新技术热点，应在基础研究、方法和模型建立、可信度等多方面同步考虑不确定性带来的风险问题

人才层面

- 工业企业普遍安全意识不够；融合场景下的风险防范意识更是缺失
- 加快复合型人才培养





04 思考和展望

政策层面

工业安全和网络安全还是相对独立的两套体系在运行，需尽快打破边界限制，建立统一的运行、监管机制；

顶层规划和生态环境建设

- 推动智能化网络化融合环境下的工业安全技术体系、标准体系、法律法规、人才队伍、政策策略、组织机构等的规划建设和协同发展；
- 推动基础科研、技术开发、工程实施、运维应用、测评认证、监督管理等机构间的安全一体化协同；
- 推动风险分析、安全需求、设计开发、工程集成、运行管理、维护变更等安全生命周期各阶段间的安全一体化协同；
- 加强国际间交流与合作，以推动国内外在技术发展和标准化建设等方面的协同





工业控制系统
信息安全产业联盟
Industrial Control Systems Information Security Industry Alliance

Thanks