TUV南德专家解析“ 自适应物理安全与信息安全系统 ”应用场景

实现智能制造安全性的动态方法

北京2023年4月26日 /美通社/
-- TUV南德意志集团（以下简称"TUV南德"）发布的"自适应物理安全与信息安全系统"（Adaptive Safety & Security System，简称AS3）提出了面向智能制造的动态风险评估方法，实现工业4.0系统运行时的监控，安全措施自动验证和系统变化的动态确认。本文中TUV南德专家以几种含有AGV/AMR的典型智能工厂场景为例，详细分析了AS3系统在智能制造领域的应用。

AS3系统在智能制造领域的应用

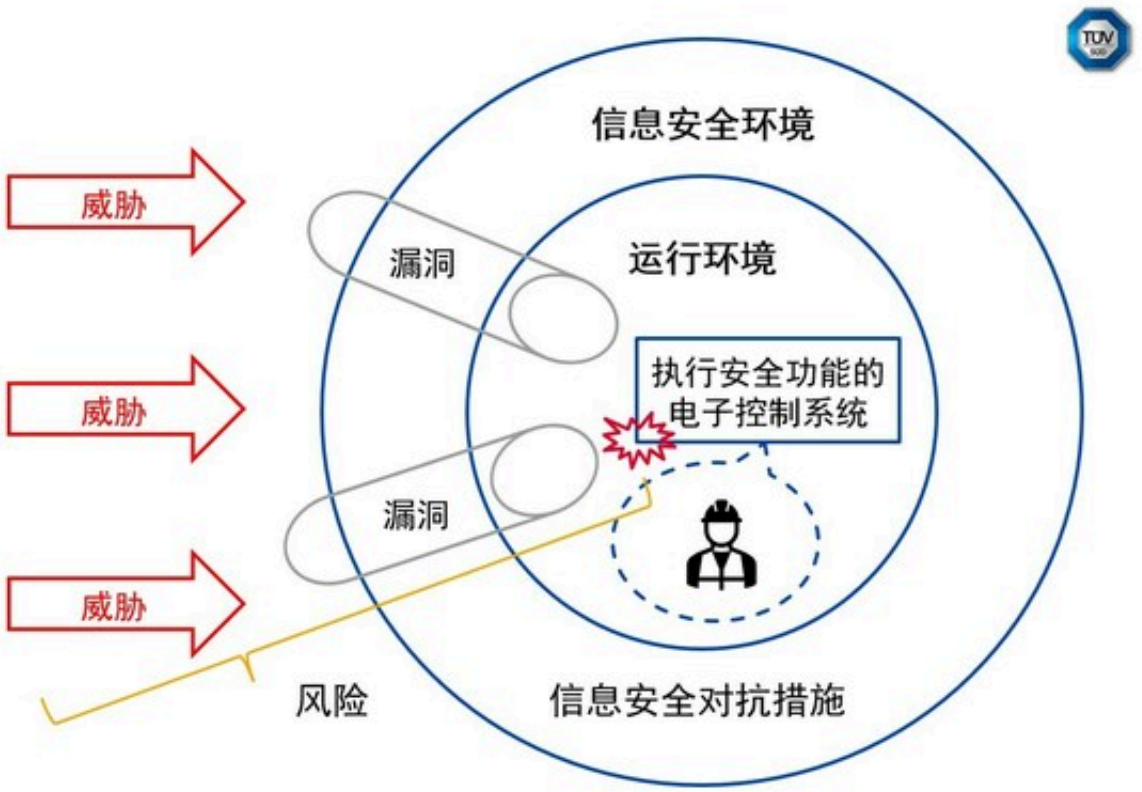
本系列文章的上篇通过两个示例展示了AS3在智能工厂中应用的部分优势：

- 通过安全措施的自动验证实现流程优化
- 通过系统变化的动态确认减少停机时间

本篇中TUV南德专家将进一步从信息安全的角度分析AS3在智能工厂以及过程工业中的潜在应用。

在进入具体场景分析之前先简要介绍一下工业信息安全标准及其风险评估。现行的国际工业信息安全标准是IEC 62443系列，包括通用、策略与流程、系统、部件（产品）等四个层级。从产品供应商的产品开发，到系统集成商进行系统集成，再到资产所有者或服务商的运行维护，所有利益相关方都可以从流程和技术两个方面参考IEC 62443标准的要求。

虽然IEC 62443标准构建了工业信息安全体系的完整框架，但是由于智能工厂日益增加的复杂性，资产所有者和运营方在智能工厂信息安全的实践依旧十分困难。特别是智能工厂中越来越多的使用带有通讯功能的电子控制系统，当信息系统存在漏洞，通过网络攻击可以使电子控制系统的安全功能失效，从而造成人身伤害或财产损失。因此物理安全/功能安全与信息安全结合的风险评估需要在两个领域都有丰富经验的专家来完成。



交织的信息安全与物理安全

对于以上困境，AS3系统是一个有效的解决方案。除了物理安全档案(Safety profile)，AS3还为智能制造系统的数字孪生配备了定制化的信息安全档案（Security Profile）。以信息安全档案中表征系统漏洞、威胁、对抗措施和风险的静态或动态参数为输入变量，推理引擎会根据实际应用的约束条件来运算，判定场景是"安全/非安全"状态，从而在运行时（@Run-time）或在系统变更时自动进行信息安全风险评估和安全确认。

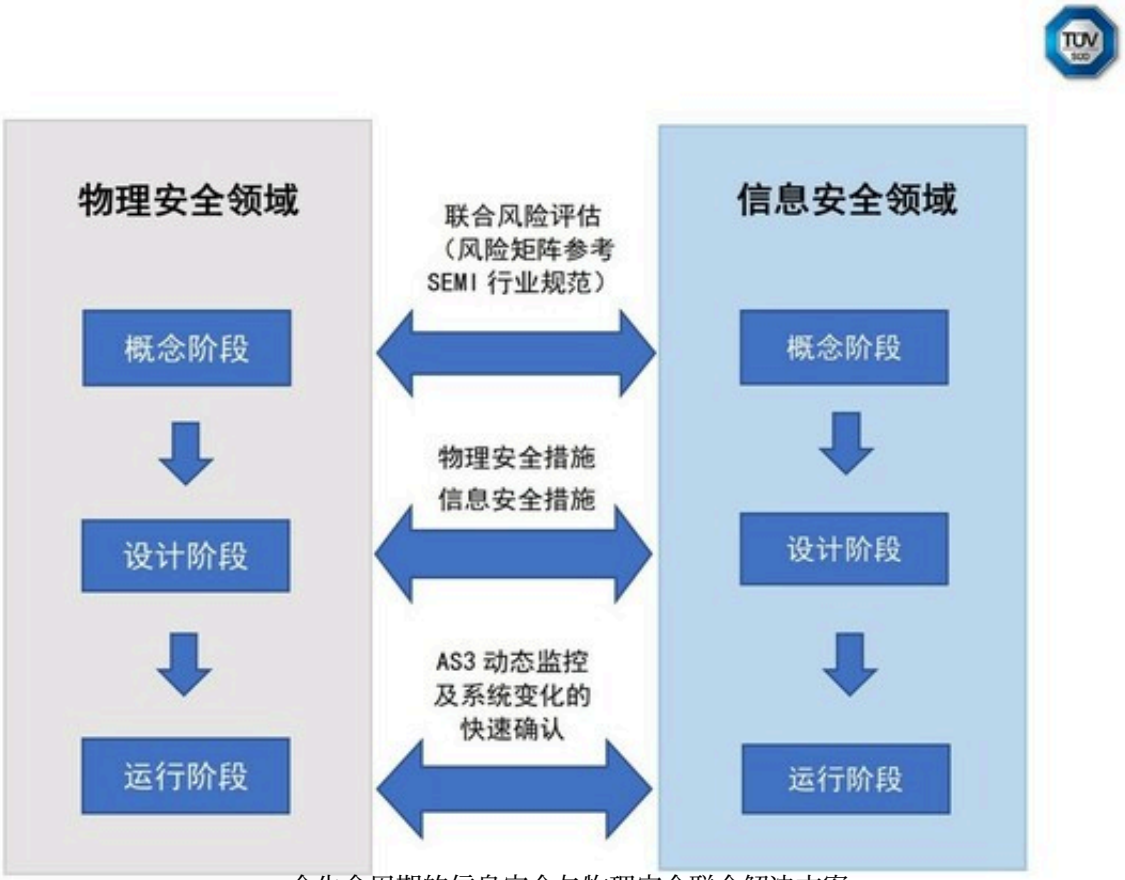
特别需要强调的是，AS3的安全档案同时嵌入了信息安全的领域知识和物理安全的领域知识及TUV南德专家丰富的信息安全与物理安全结合的风险评估实践经验。AS3的动态风险评估方法可以有效的帮助运营方及系统集成商应对智能工厂日益复杂的风险图景。

示例3：信息安全与物理安全/功能安全的联合评估

某芯片制造工厂运行一批UR的移动式协作机械手IMR，这些IMR在移动作业时可能进入不同物理安全风险等级的区域，并且在不同的位置可能会与分布于不同区域的无线接入装置（无线AP）连接，并通过不同的路由器接入工厂信息系统。工业信息安全分区与物理安全分区有所不同，物理安全分区是按连续空间划分的，而信息安全分区中的资产是按互联逻辑划分的，因而IMR在移动作业时可能进入不同风险等级的物理安全区域和划入不同风险等级的工业信息安全区域，两者又不是对应的。情况非常复杂。

在系统集成时(T0)，TUV南德的信息安全专家基于SEMI行业规范和工业信息安全标准对这些IMR及其相关IT设施进行了信息安全风险评估，并建立了信息安全档案。与此同时，TUV南德的物理安全专家基于SEMI行业规范和物理安全标准建立了物理安全档案。AS3与工厂MES制造管理系统连接，在工厂运行时可以持续地对这些IMR及其相关IT设施，生产设施进行信息安全和物理安全的动态监控。

在建立该工厂信息安全档案的过程中，TUV南德由信息安全专家，功能安全专家及SEMI评估专家组成的工作组还执行了联合风险评估，评估过程中综合考虑IMR移动到不同作业区域可能出现的机械安全风险，包括潜在的人身伤害和财产损失（需考虑SEMI行业特殊的财产损失评估规范），以及在这些作业区域运行时无线接入到不同的信息安全分区，和各种可能场景下的信息安全风险，并对所有场景都分别确定了具体的信息安全要求以及满足要求的条件。



全生命周期的信息安全与物理安全联合解决方案

工厂运行时AS3将提供动态监控，并在系统出现变化时提供在线风险评估以快速确认变化是否可以接受或给出安全措施的建议。由此显著减少智能工厂因系统变更造成的停机时间，提高生产率，并提升工厂运行的灵活性。目前，AS3已经由TUV南德香港分公司申请专利保护。

原文地址：http://www.china-nengyuan.com/news/194647.html