



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

工业控制系统网络能否实现极限安全？

解读中国科协2019工程技术难题之一

汇报人：东南大学、冷杉
汇报日期：2019年5月9日

中国科协科学和工程问题征集评选



- ▣ 研判未来科技发展趋势
- ▣ 抓住科技创新突破口
- ▣ 前瞻谋划和布局前沿科技领域与方向提供依据
- ▣ 推进世界科技强国建设



中国科协重大科学问题和工程技术难题征集评选系统

www.scique.cn/site/ProjectRecruit.jsp

01 完善信息 02 项目填报 03 后台审批 04 审批结果

申报流程

学会提交人 完善学会信息 学会提交人 填写项目信息 项目组 进行后台审核 通过 进入投票环节 退回 退回学会提交人修改

学科领域

数理科学 化学科学 生命科学 地球科学 工程与材料科学

信息科学 医学科学 管理科学 其他

中国科协重大科学问题和工程技术难题征集评选系统

16°C 21:42 2019/4/27

信息科学类科学问题和工程难题

□2018年度公布有6项

- 类脑计算
- 认知物联网
- 抗量子密码算法设计
- 无人运载工具仿真
- 工业互联网
- 人机情感交互

□2019年度申请进入第二轮有63项

- 本难题，由中国自动化学会提交申请
- 是唯一涉及网络安全的难题



本工程技术难题的题目

□中文题目：工业控制系统网络能否实现极限安全？

□英文题目：Can We Achieve Ultimate Cyber Security in Industry Control System

本工程难题关键词的确定

□工业（运行，重要性，占比）

- 连续制造工业——能源、石化、冶金

- 社会基础设施——电力、核能、交通、水利、环保

□控制系统（底层的，人机混合，存量）

- DCS

- SCADA

- PLC

□网络（处理器、操作系统、通信、软件、数据库）

- 网络安全

本工程难题的核心

□提出**极限安全**概念

□指出解决方案

工业控制系统网络安全面临严峻挑战

- ❑ 安全漏洞不断增多，安全威胁加速渗透，攻击手段复杂多样
- ❑ 可能引发涉及电气安全、压力容器安全、化学物质安全、甚至核安全等严重事故
- ❑ 会导致人员生命、基础设施和生态环境等不可挽回的损害。

工控网络安全重要性

- 国家总体安全战略重要组成部分
- 法律法规等密集出台
 - 信息安全法
 - 行动计划
 - 指导意见
- 涉及重要部门
 - 工信部
 - 科技部
 - 公安部
 - 发改委、能源局
 - 央企集团
- 安全问题渗入所有新技术革命板块
 - 云计算、大数据、物联网、人工智能、移动通信
 - 自动控制系统、信息管理系统、工业4.0、工业互联网、中国制造2025

追求目标陡然增加

- 原来，工业控制系统设计、研发、制造、部署所追求的目标：
 - 完善控制功能
 - 保证实时性
 - 提高控制效率
 - 克服随机扰动

- 在引入网络安全威胁之后，就需要增加应对由恶意智力带来的：
 - 不确定性
 - 不可知性
 - 多变性

工控安全现状堪忧

- ❑ 工业领域核心的控制技术开放度极高
- ❑ 工业控制系统长期依赖进口，大量装备了国外系统
- ❑ 因为有供应商依靠，造成了工控安全意识薄弱，安全责任旁落，安全防护缺失
- ❑ 工控信息安全产业刚刚起步

工业控制系统网络安全难点痛点

- 局限于信息网络安全技术的衍生
- 工业互联和安全的原始性冲突
- 庞大的系统存量
- 对实时的高要求
- 对介入控制回路的敏感性
- 不能忍受频繁升级

关注和思考绝对网络安全

- 无论中国的，外国的
- 开发机构，业主用户
- 政府领导层、企业管理层、基层技术人员
- 出于常识、理性、视野、远见，还是责任担当，都会思考
- “终极安全”？“绝对安全”？不存在

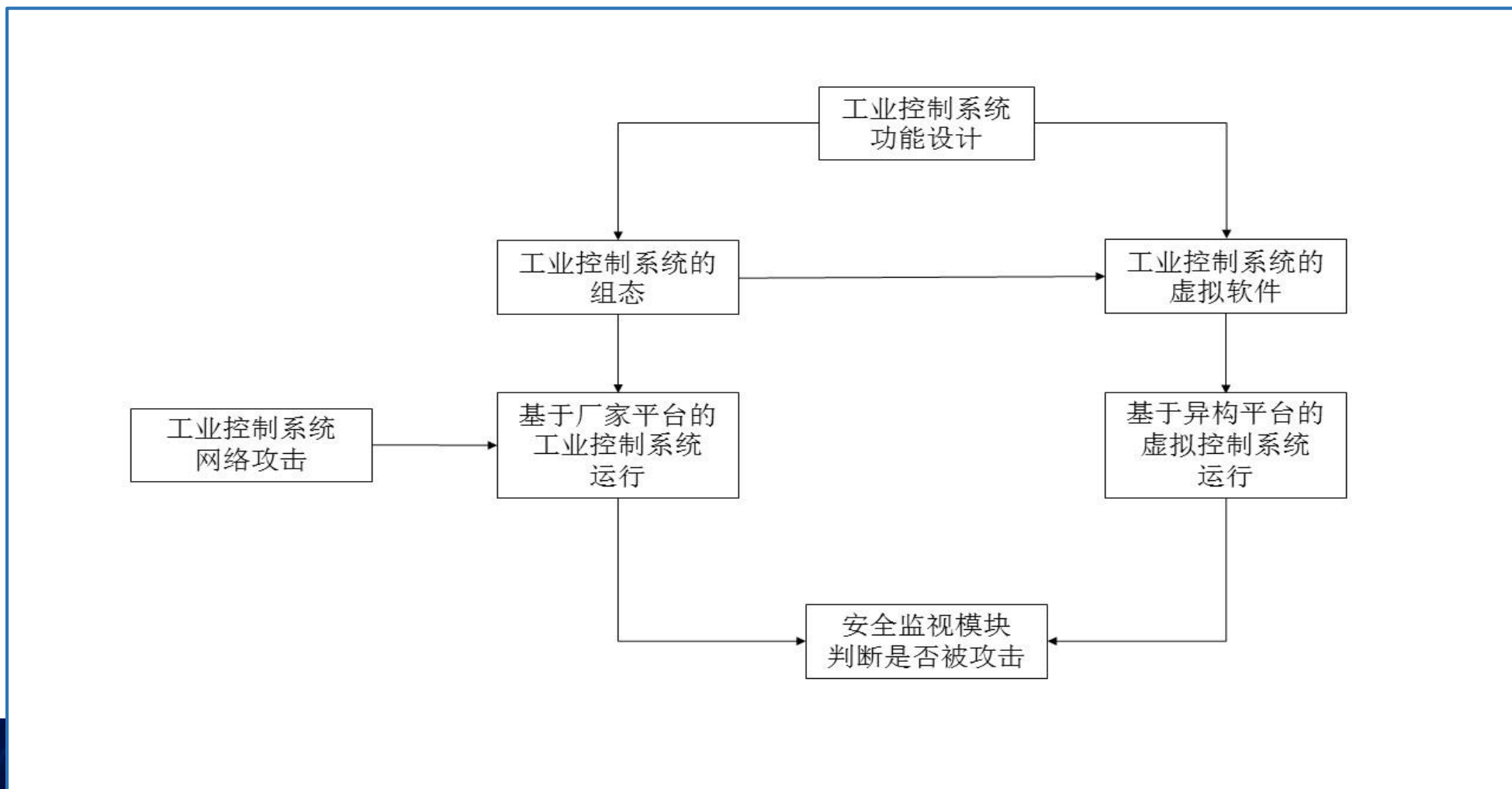
首次提出工业控制系统网络极限安全概念

- 采用工程技术的方法
- 实时感知到恶意智力给网络带来的不确定性、不可知性和多变性
- 将工业系统最终导向安全运行
- 实现工业控制系统网络的极限安全
- 属于现实的未解决的工程技术难题

对工业控制系统网络零信任

- 工业控制系统是按照确定的组态实现控制的
- 但在网络威胁下，只能是“永不信任，始终验证”
- 引入完全可信任的**虚拟控制系统**进行监视验证
- 首次提出解决难题的思路方法

首次提出引入虚拟控制系统实现极限安全



曾首次提出虚拟控制系统

- ❑ 2003年，在“中国电力”论文“论虚拟分散控制系统技术”
- ❑ 虚拟DCS是相对于在过程工业系统中运行的真实DCS而言的，虚拟DCS就是将真实DCS在非DCS的计算机系统中以某种形式再现。虚拟DCS就是要在一种通常为开放平台的计算机信息管理系统中，尽可能真实地再现分散控制计算机系统。
- ❑ 虚拟DCS的特点是控制参数和算法完全来自于下载文件，使用与DCS相同的算法、模块、时间片、位号等，可同步修改更新，软件功能逼真度很高。

在“知网”检索“虚拟控制系统”

浏览器地址栏: kns.cnki.net/kns/brief/default_result.aspx

搜索框: 虚拟控制系统

检索结果: 28条结果

排序: 相关性 | 发表时间 | 被引 | 下载

已选文献: 0

题名	作者	来源	发表时间	数据库	被引	下载	阅读	收藏
21 基于虚拟样机的机器人控制仿真软件系统研究与开发	陈新荣	北京工业大学	2003-05-01	硕士	14	799	799	☆
22 电力驱动系统实时控制虚拟实验平台	卢子广; 柴建云; 王祥珩; 苏鹏生	中国电机工程学报	2003-04-30	期刊	99	752	752	☆
23 直流电机计算机控制综合平台驱动模块及控制软件设计	王力刚	西北工业大学	2003-03-01	硕士		492	492	☆
24 基于Simulink和虚拟现实工具箱的机器人行驶控制系统计算机仿真	王建中; 胡光艳; 田会方	国外建材科技	2003-02-28	期刊	6	393	393	☆
25 虚拟企业环境下企业生产计划与控制系统的研究	王扶东; 薛劲松; 朱元龙; 李兵; 李莉	计算机工程与应用	2003-02-24	期刊	21	298	298	☆
26 论虚拟分散控制系统技术	冷杉	中国电力	2003-02-20	期刊	92	216	216	☆
虚拟仪器及控制在自动化测试系统中的应用	马金萍	质量天地	2003-02-15	期刊	1	62	62	☆

工业控制系统信息安全产业联盟 ICSISIA

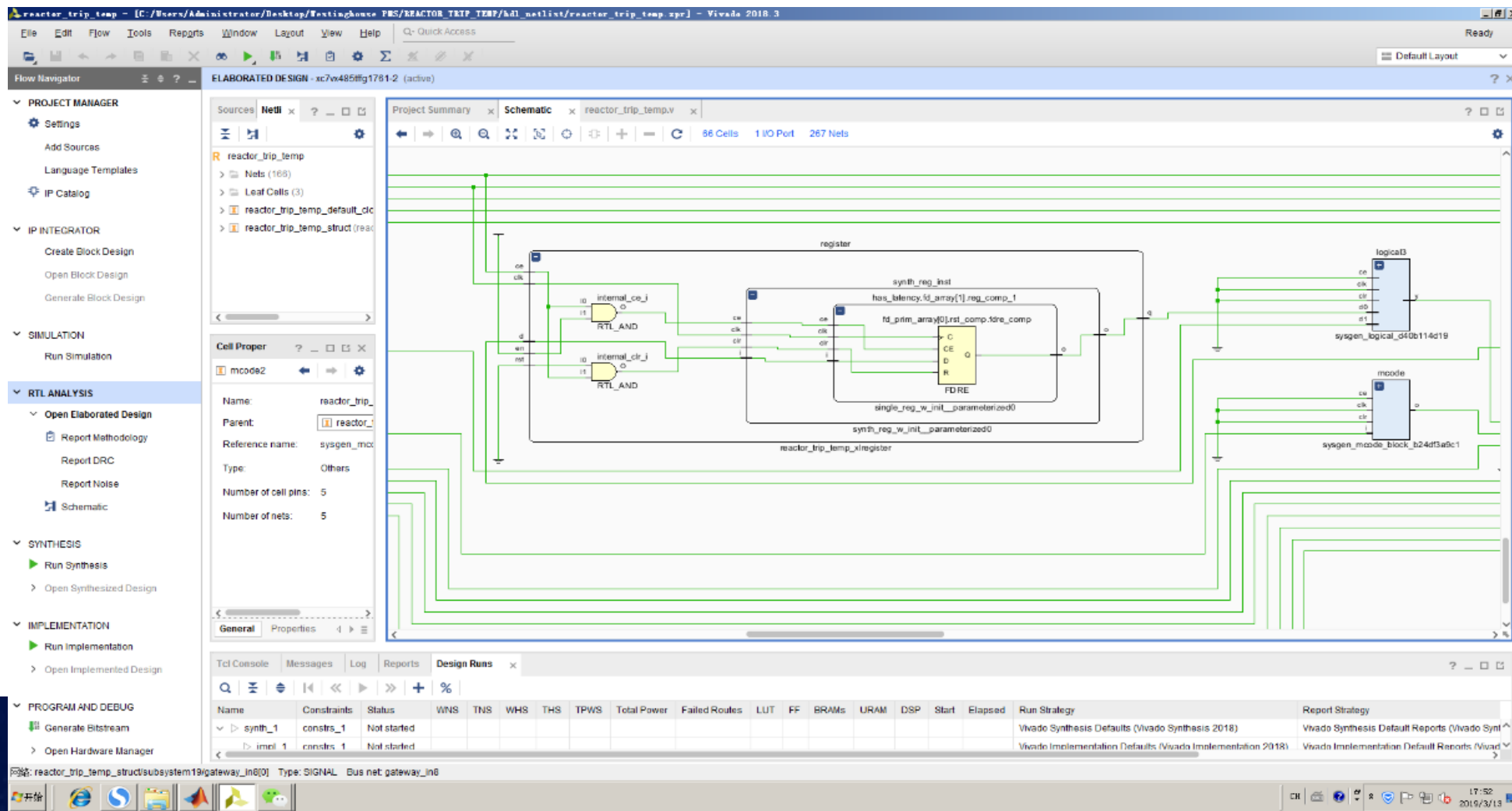
曾长期研发虚拟控制系统

- 团队共发表虚拟控制系统技术相关论文23篇
- 覆盖性深入研究多种DCS系统
- 开发多种虚拟DCS软件系统

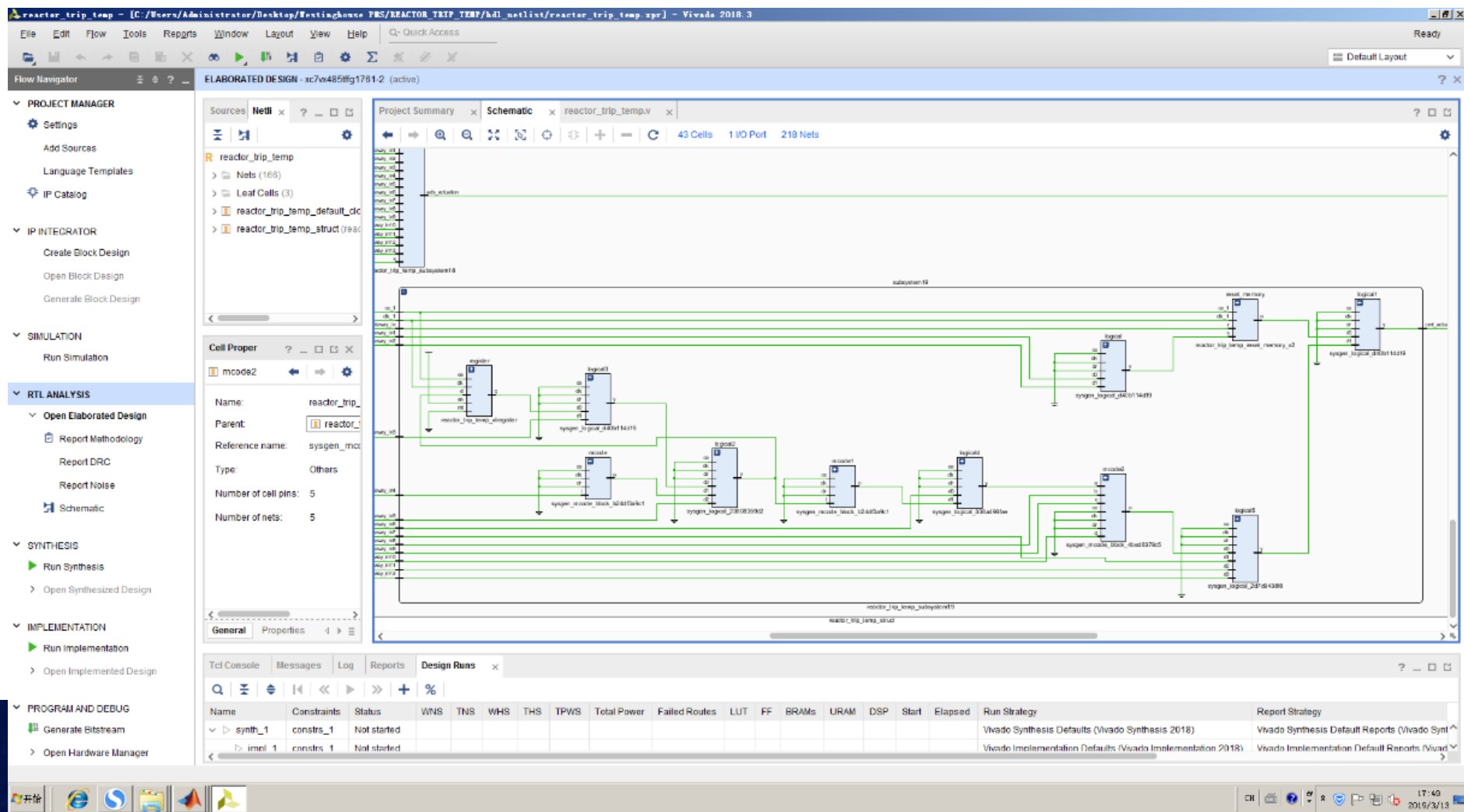
首次提出异构平台实现虚拟控制系统

- ❑ 基于异构平台（Heterogeneous Platform）解决网络安全难题
- ❑ 采用现场可编程门阵列FPGA（Field Programmable Gate Array）技术方案实现虚拟控制系统
- ❑ 自主知识产权，已经实施实验室开发

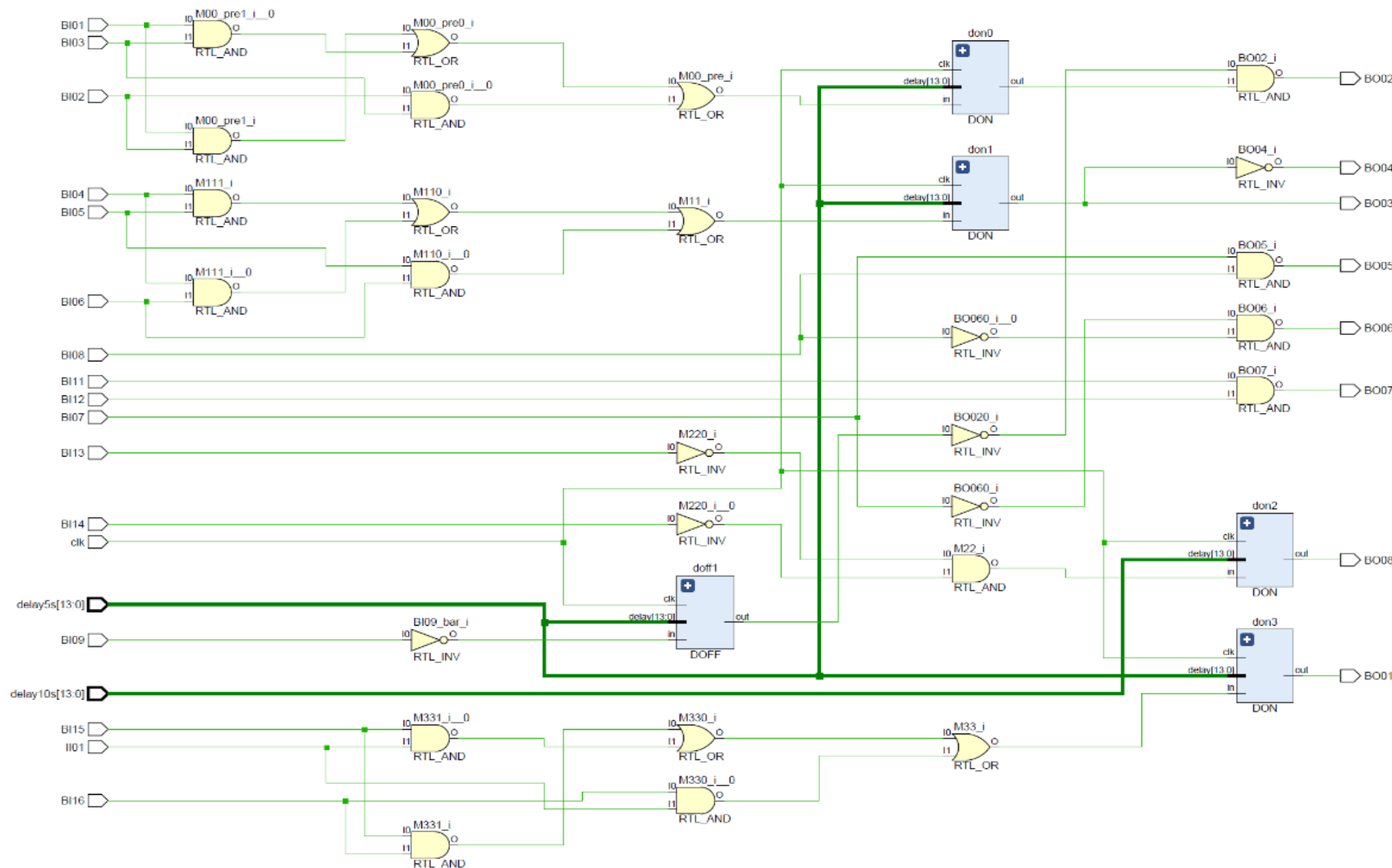
核反应堆安全控制——FPGA虚拟跳堆



核反应堆安全控制——FPGA虚拟跳堆



火电厂锅炉控制——FPGA虚拟主燃料跳闸



基于异构平台虚拟控制系统实现工业控制系统网络极限安全

- 欢迎合作研究
- 欢迎支撑实验室开发
- 欢迎委托落地试点应用



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

Thanks