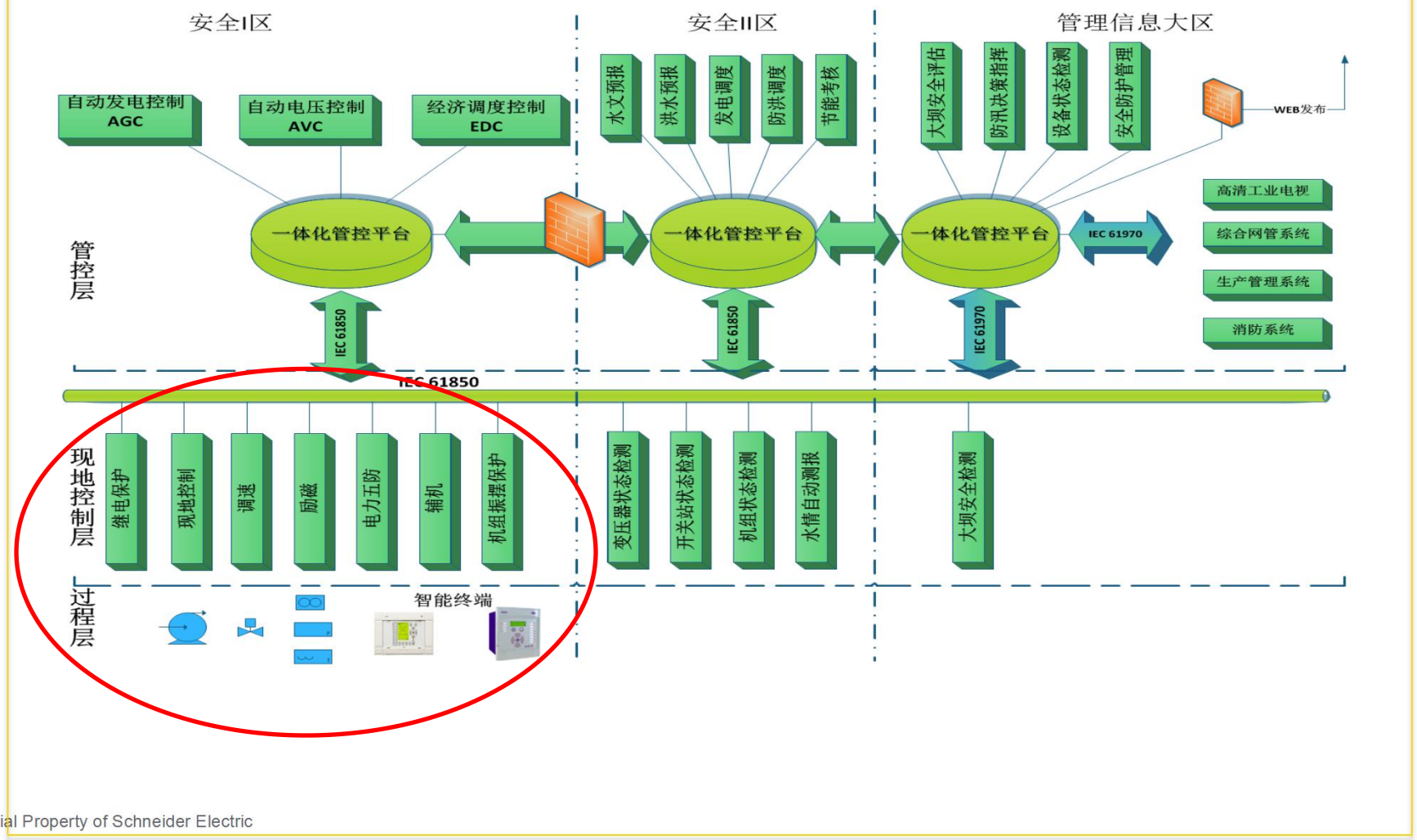
构建信息安全的PLC系统

梁军
信息安全负责人
施耐德电气工业事业部

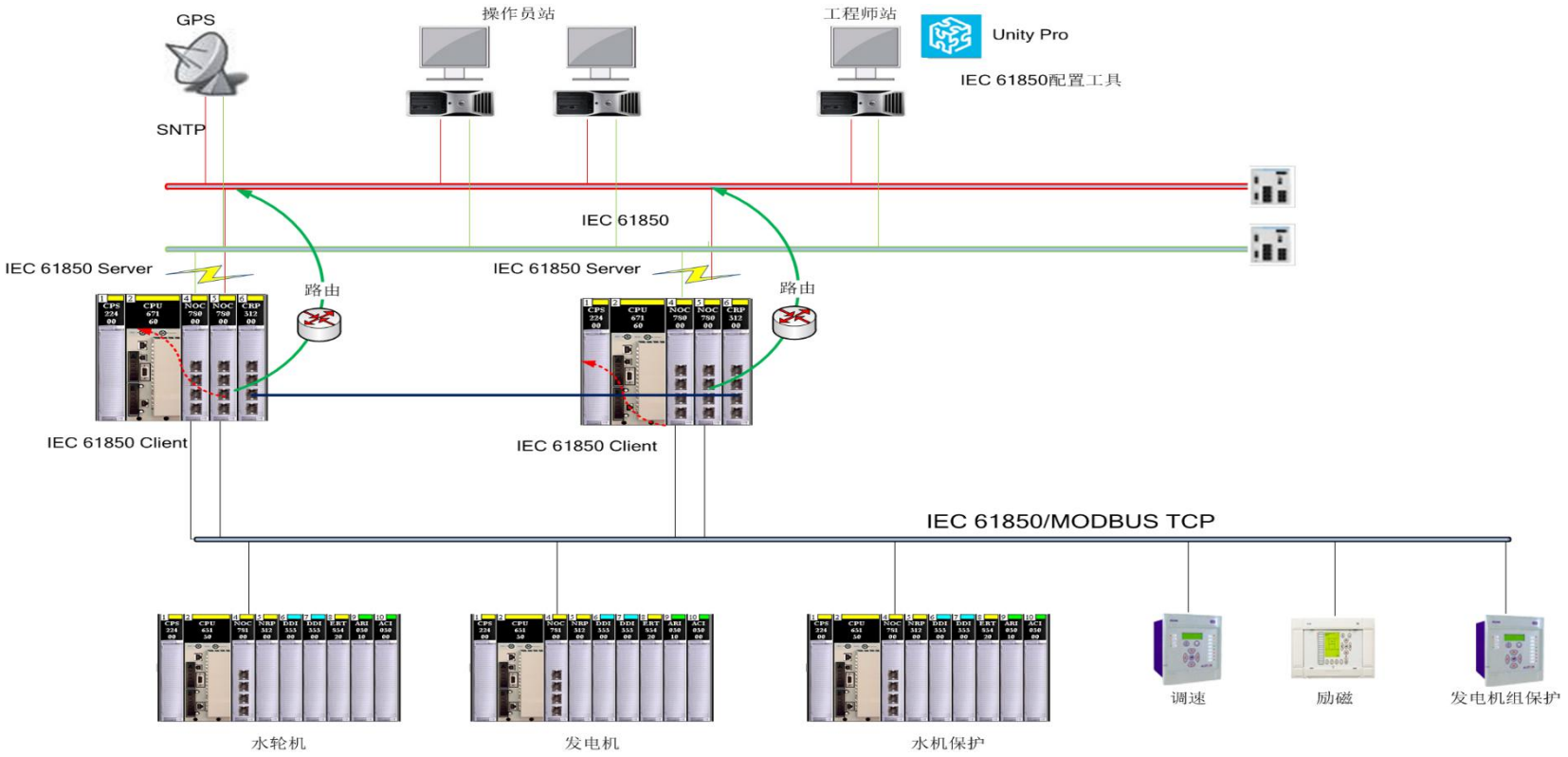
Life Is On Schneider Electric 施耐德电气

智能水电系统

系统架构图



基于工业以太网架构的数字化的PLC系统



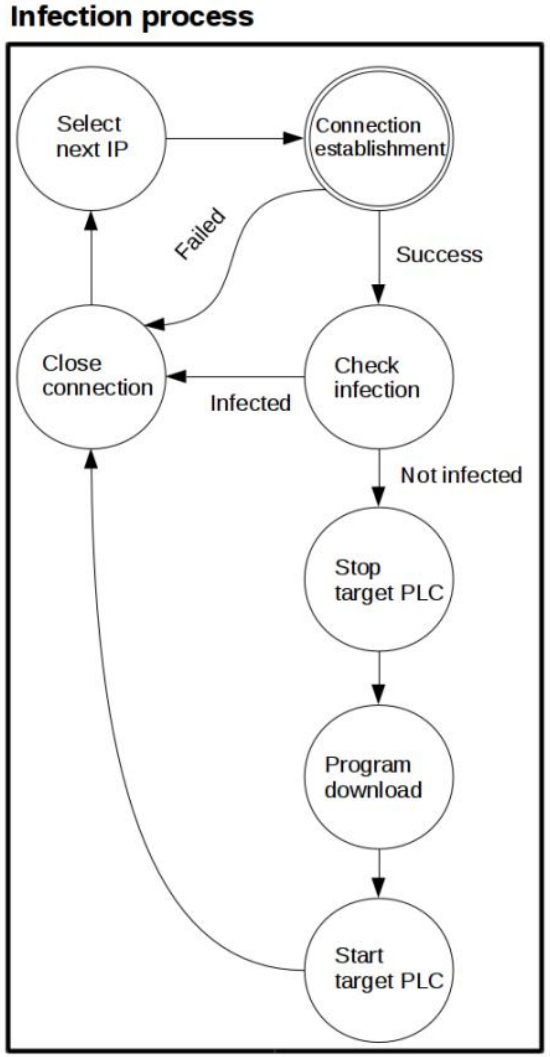
工业控制系统信息安全风险

- 穿透网络边界的渗透攻击
- 来自移动设备和临时接入设备的内部病毒感染
- 网络风暴、网络设备故障、异常通信等造成的网络和设备失效
- PLC之间的病毒传播

PLC病毒

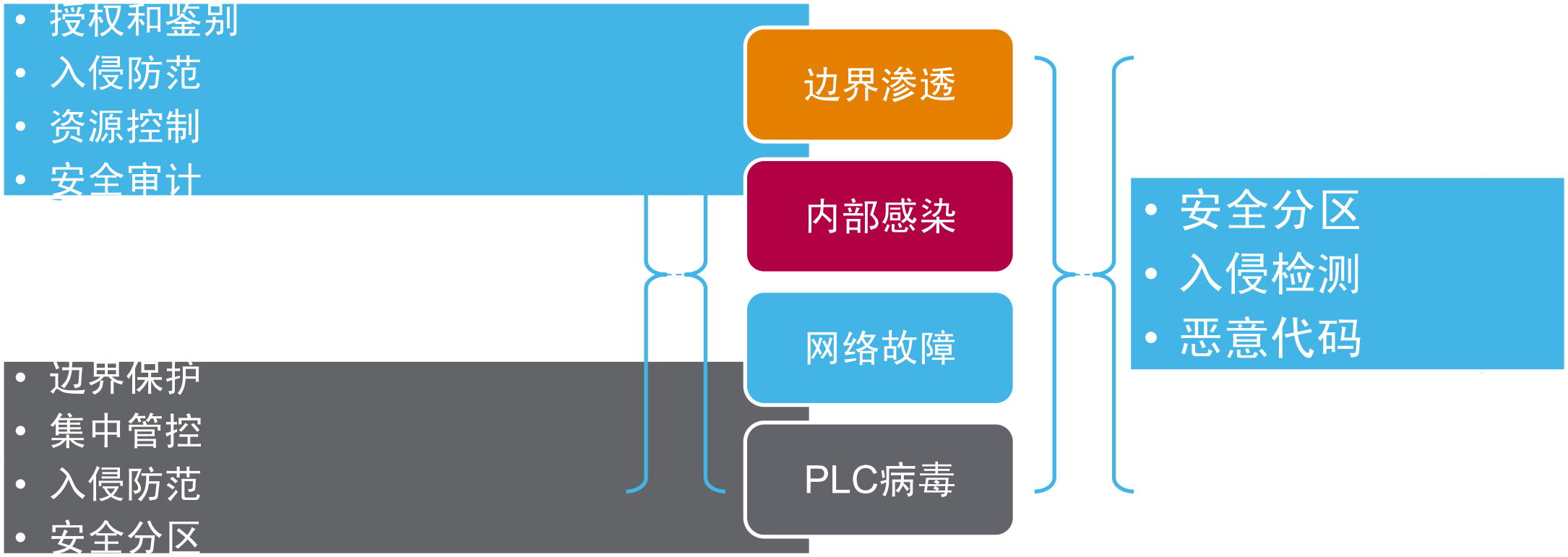
PLC 程序

PLC 固件



https://regmedia.co.uk/2016/04/29/plc_87458745.pdf

信息安全防护与合规



能源局
36号文

施耐德信息安全

通过3个维度为客户建立安全的控制网络:

- 产品(图中橙色圈)

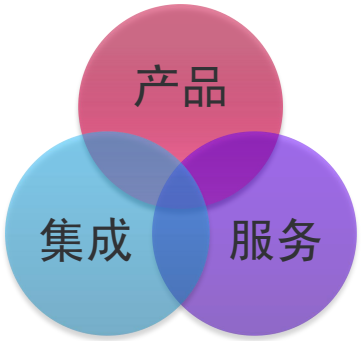
  自身具备信息安全能力和认证的PLC(M580) DCS(EVO)产品

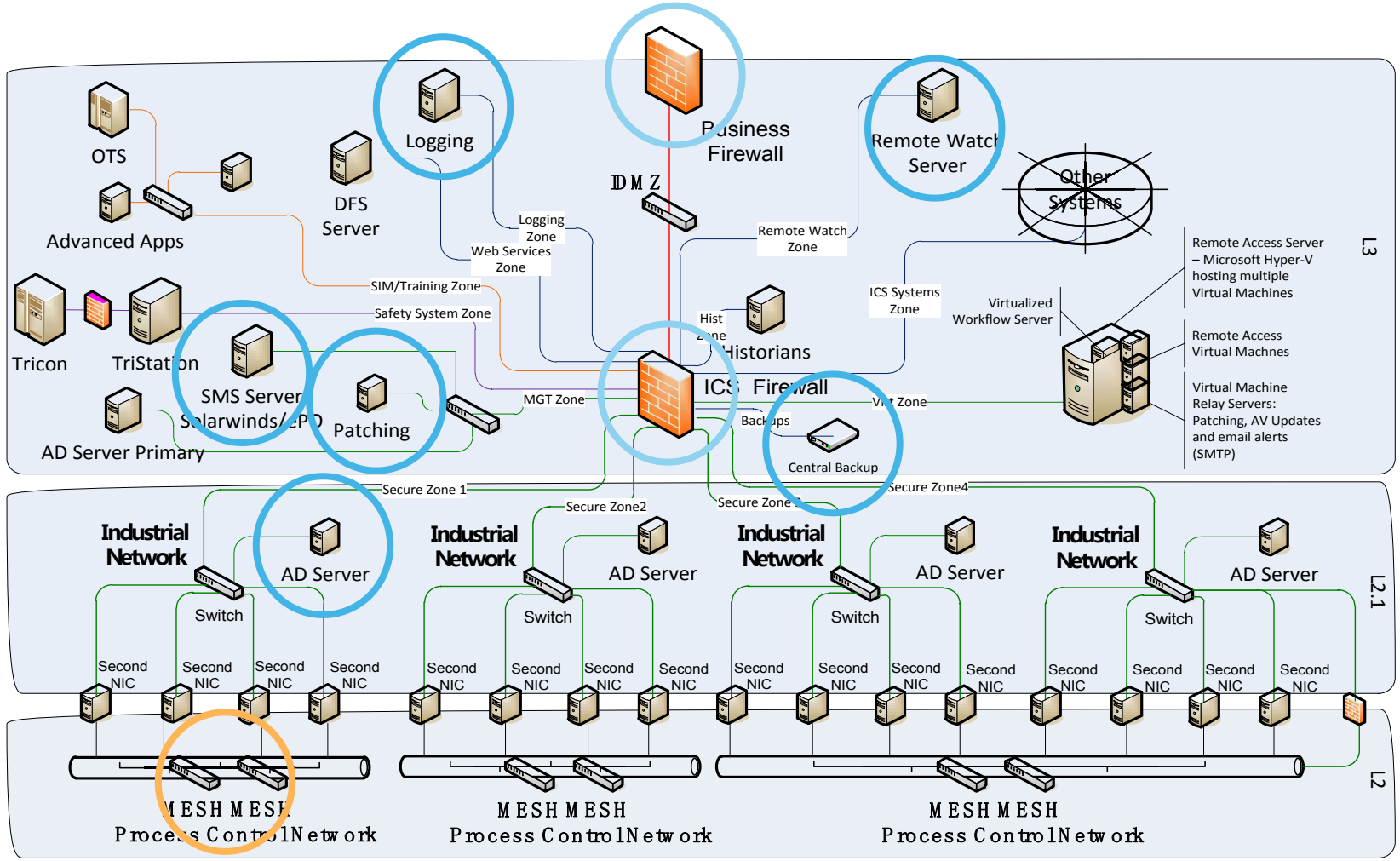
- 项目集成(图中蓝色圈)

  在控制网中植入国家权威机构认证的防火墙/杀毒软件/监控审计/灾备等信息安全产品来构建防御/预警/恢复等多维度的纵深安全体系

- 服务

  信息安全项目实施投运后的一系列信息安全分析/维护/培训/病毒库和补丁更新等持续性服务





产品：新一代昆腾+PLC信息安全设计

相生相伴的PLC信息化与信息安全

全新的Modicon M580—真正做到“E网到底”的ePAC，灵活的以太网架构，实现无限可能

全生命周期的信息安全

- IPSEC加密授权通信，屏蔽指定设备外的任何通信
- 数字签名与加密存储双保险的固件文件
- 基于IP的单机或子网身份认证
- 可追溯，关键操作/状态的日志上传
- IO网络与监控网络物理隔离

客户价值导向

- 根本上增强安全性，覆盖外围安全产品的盲点
- 满足国内外所有标准和等级保护的要求
- 自身集成的安全性可取代部分外围专业安全产品，大幅降低设备投资的同时减少系统的故障点

产品：施耐德PLC产品信息安全认证

Certificate Of Compliance

This is to certify that the:

Modicon M580 BME P58 3020

Manufactured by:

Schneider Electric

Is in compliance with the requirements set forth by:

Achilles Level II Certification

This certificate is restricted to the specified version of the referenced Device (including model number, hardware/firmware/software version, and control protocols) set forth in this Certificate. Any change to the Device might impair the Device's ability to pass the standards referenced in this Certificate. This Certificate is based upon limited testing, and is not a complete or comprehensive certification of the security of the Device. The Device may contain security vulnerabilities and deficiencies that are not covered by the standards referenced in this Certificate. This Certificate is subject to revocation by Wurldtech Security Technologies Inc.

More information regarding this Certificate and the Achilles Level 1 Standard is available at www.wurldtech.com and upon request from Wurldtech Security Technologies Inc.

CERTIFIED achilles CERTIFIED

CERTIFICATE NO. CERT-152-161213

PV: 01
HARDWARE VERSION

V1.xx
FIRMWARE VERSION

N/A
CONTROL PROTOCOL

Embedded Device
CATEGORY

Nate Kube, CTO

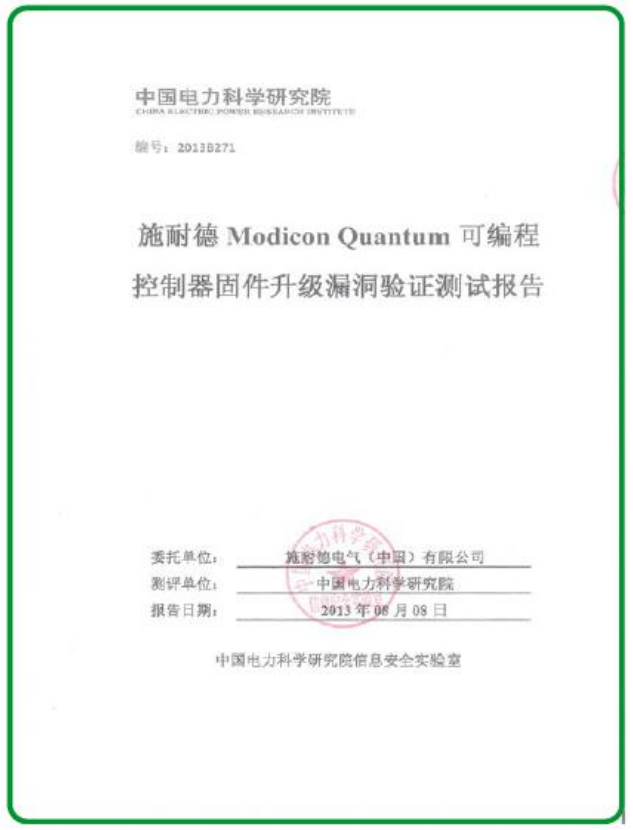
wurldtech
security technologies

编号：RW-332/1207-12CJ14

信息技术产品安全性复测报告

产品类型：硬件产品
产品名称：施耐德莫迪康昆腾系列PLC
送检单位：施耐德中国

国家信息技术安全研究中心
二〇一二年八月三十一日



中国电力科学研究院
CHINA ELECTRIC POWER RESEARCH INSTITUTE

编号：2013B271

施耐德 Modicon Quantum 可编程控制器固件升级漏洞验证测试报告

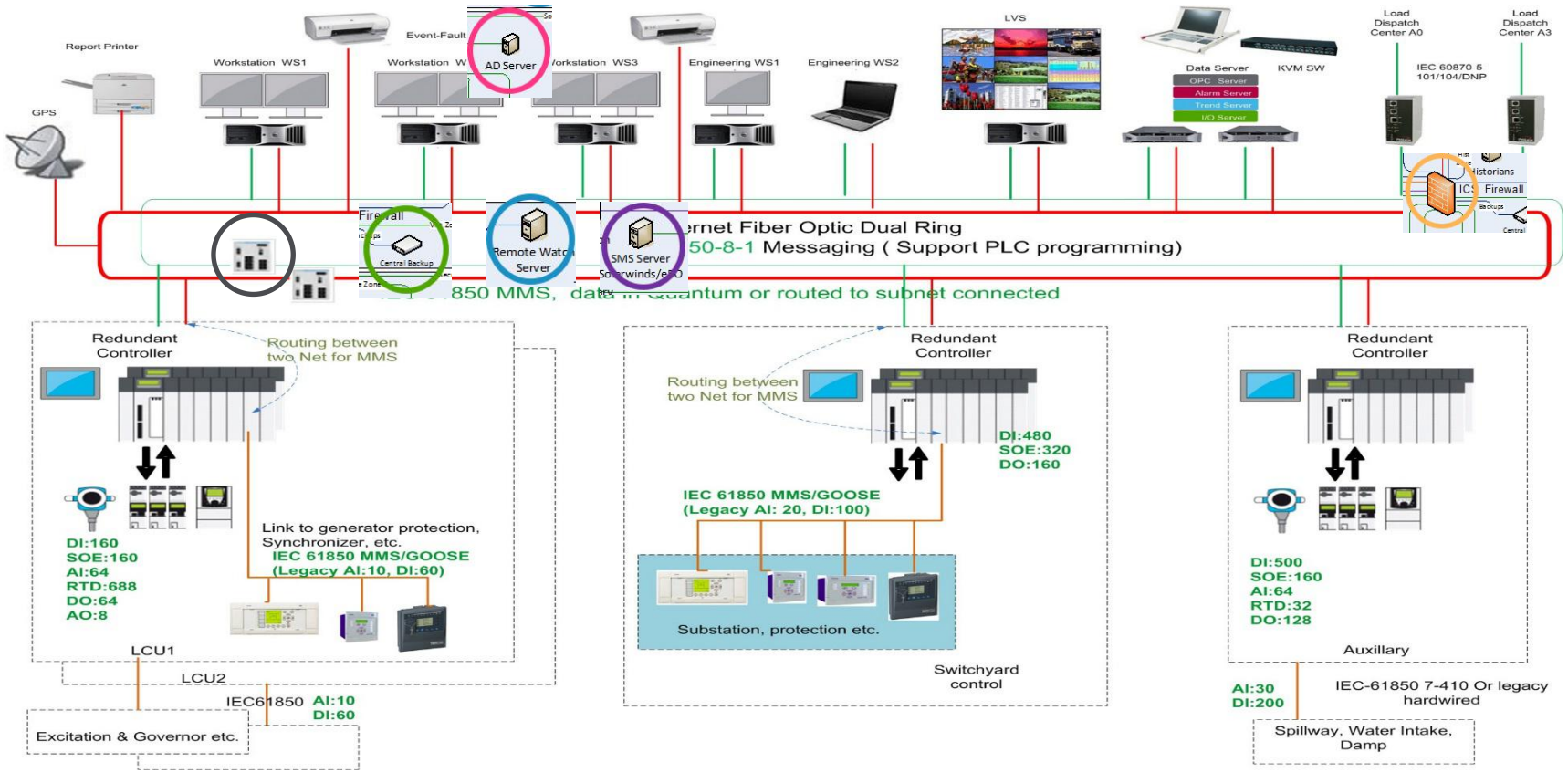
委托单位：施耐德电气（中国）有限公司
测评单位：中国电力科学研究院
报告日期：2013 年 08 月 08 日

中国电力科学研究院信息安全实验室

- 自2015年起新上市的所有产品将满足Achilles认证和任何国家级标准

集成：控制系统信息安全

- 安全分区
- 入侵检测
- 恶意代码
- 安全审计
- 灾难备份



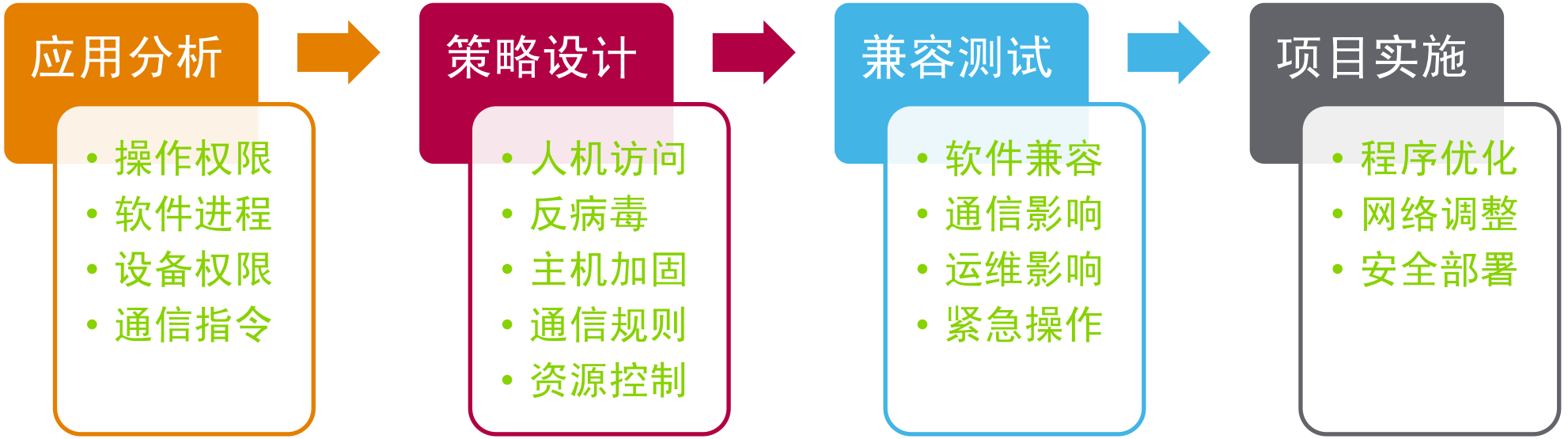
- 授权鉴别
- 入侵防范
- 资源控制
- 安全审计

- 边界保护
- 集中管控
- 入侵防范
- 安全分区

粉色安全域- 恶意代码防范+主机加固+授权鉴别；
紫色网络监测 - 入侵检测+集中管控；
黑色管理交换机 - 安全分区+资源控制；

橙色防火墙 - 边界保护+入侵防范；
蓝色审计平台 - 安全审计；
绿色灾备系统 – 灾难备份；

集成：控制系统信息安全



*完美的安全构建需要“精通系统应用及工艺”、“熟悉PLC产品及编程”、“信息安全部署能力”相结合

施耐德信息安全部分业务案例

中东

- 信息安全 / DCS / Safety 系统 (存量及新建)

  卡塔尔和阿布扎比的油气公司

  阿曼的石油公司和炼油厂

非洲

- 信息安全 / DCS 存量系统升级 / Safety 系统升级

  尼日利亚和埃及

东亚

- 信息安全 / DCS 新建项目 for 新加坡
- 信息安全

  马来西亚海上油田

北美

- 信息安全 / DCS 升级 / Safety 系统升级

  美国多家炼油厂

  美国多家电力公司

- 信息安全

  美国核电厂

欧洲

- 信息安全 / DCS 升级 / Safety 系统升级

  德国和比利时炼油厂

- 信息安全 / DCS 新建项目 for 瑞士
- 信息安全

  俄罗斯多家核电和天然气工厂

攻防演练显身手

国家能源局电力安监司苑舜副司长

公安部信息安全等级保护评估中心副主任毕马宁

China Power 中国电力 .com.cn

全国首届工控系统信息安全攻防竞赛圆满闭幕

2015年11月23日13:34 作者：中国电力网

本次赛事采用施耐德Quantum PLC搭建火电厂生产环境，在系统中预留出若干漏洞，参赛选手在仿真环境中展开攻击。。预赛系统，仿真投运时间较长、系统安全防护措施差的生产环境，所有参赛选手在短时间内都有所斩获。通过预赛，印证了部分存量工控系统存在漏洞，缺少有效的防护措施。排位赛结束后，中国科学院信息工程研究所、国网智能电网研究院信通所、北京威努特技术有限公司、国家互联网应急中心获得决赛权。

决赛现场

决赛环节，PLC控制系统分别布局了中级、高级安全策略，部署了中科网威的工控网络异常感知与审计系统和工控防火墙、赫思曼的工业交换机，增强了系统的安全防护性，决赛环节更具挑战性。竞赛组委会为各参赛队提供绿盟工控漏洞扫描系统作为攻击工具，经过两个多小时的鏖战，最终冠军队以PC漏洞为切入点，成功实施有效攻击，决算止步于中级防护策略。本次竞赛同时印证组委会设计的以新版PLC控制系统和专业系统防护设备为代表的安全防护策略，成功抵御专业红客的攻击行为。

http://hvdc.chinapower.com.cn/news/1039/10399678.asp

http://news.xinhuanet.com/info/2015-11/20/c_134837752.htm

一、采访对象：

本次竞赛主办单位之一、公安部信息安全等级保护评估中心　常务副主任张宇翔（以下简称：张）

张：在技术层面，从这次竞赛的决赛阶段可以看到，以新版PLC信息安全策略和外围多层次防御手段为代表、采用由点到面纵深防御理念的系统，从始至终未被攻破，体现出了极高的安全水平。可见，采用这种纵深防御理念的信息安全解决方案，是值得广大工业用户进行借鉴和实践的。

在管理层面，广大工业用户也不难得到一些启示。工业领域的信息安全风险在实际的生产环境中尽管不一定被触发，但却时刻存在，不可不防。工业用户应该主动关注这方面的工作，做到未雨绸缪、防患于未然，而不是在问题发生后再被动应对。

记：能否请您谈一谈，普通的工业用户如要想选择更符合信息安全要求的工控产品，有哪些可行的方法？

张：目前工业用户选择采购、使用更符合信息安全要求的工控产品，可以优先选择经过国家权威检测机构、行业专业测评机构检测，安全可控的工控产品，这样有利于在设备层面减少风险。

作为工业用户，更应在系统建设和整改中，关注系统整体安全性。选择安全可靠的工控设备还只是实现了信息安全防范的第一步，用户更应在加强设备安全性的基础上，采用纵深防御理念的信息安全解决方案，做好系统安全配置、选择安全加固，更全面地提升系统整体的安全性。另外除了纵深防御理念之外，在网络环境与应用场景相对单一的生产环境中，是否还可以考虑基于可信计算的相关安全解决方案。

记：本次竞赛对提升工业信息安全的整体水平有哪些积极意义？

张：提升了用户对工控信息安全的认识，直观感受到了工业控制系统所面临的安全风险，有力地揭示了此类系统所存在的安全风险。

针对目前工控设备存在安全风险的系统，我们还是可以通过完善的安全解决方案来提升系统的安全防护能力。从决赛的情况来看，“国家级”的红客队伍并没有攻克经过设备加固和安全设备防护的方案，可以让用户建立信心。

本次大赛吸引了多支专业队伍参赛，也获得了多家工业控制设备厂商和信息安全厂商在专业技术层面上的大力支持，显示出当前业界各方对工业信息安全课题的重视程度在提升；同时也表现出这些专业厂商直面工业信息安全挑战，致力提供安全解决方案的信心和决心。

Life Is On | Schneider Electric 施耐德电气