DBAPPSecurity 安恒信息

安恒十年磨一剑
只为网络更安全

火电厂工控系统纵深防护体系建设探讨

目录

Contents

PART 01

工控安全现状

1 发电厂工业网络安全隐患分析

◆SIS系统与电厂DCS或PLC之间OPC通讯安全隐患

◆控制系统厂商的维护接入带来的安全隐患

◆控制系统与第三方系统连接，APC先控站的潜在风险

◆DCS或PLC系统各个控制站之间的互相感染隐患

2 发电厂工业网络与信息系统主要的安全威胁分析

- ◆网络风暴
- ◆主动入侵风险
- ◆外部网接入危险
- ◆漏洞利用风险
- ◆行为抵赖风险
- ◆针对特定工控系统的攻击

3 关于电厂热控工程师的信息安全培训

◆关于工业网络及协议：工业以太网、现场总线、OPC

◆关于信息安全技术：概念、攻击类型、漏洞、安全检查技术、防护技术等

◆关于安全政策和标准：14号令和36号文、工控安全指南、各种政策和标准的解读

◆工控安全认证工程师：网络安全协调小组、配合监管、工控补短板，以防安全厂商忽悠

4 关于电厂控制系统日常管理

◆关于USB口管理，比较严格

◆关于交换机空闲端口禁止、MAC地址绑定

◆关于工控网络的VLAN

◆准入控制如何做到位？（及时发现非法接入）

5 关于电力监控系统36号文：完善

◆重视边界防护，但没有深刻理解

◆ 分区分域：生产大区和管理大区，生产大区控制系统如何分，如何做好各控制系统之间的隔离（VLAN、传统防火墙、工业防火墙？）

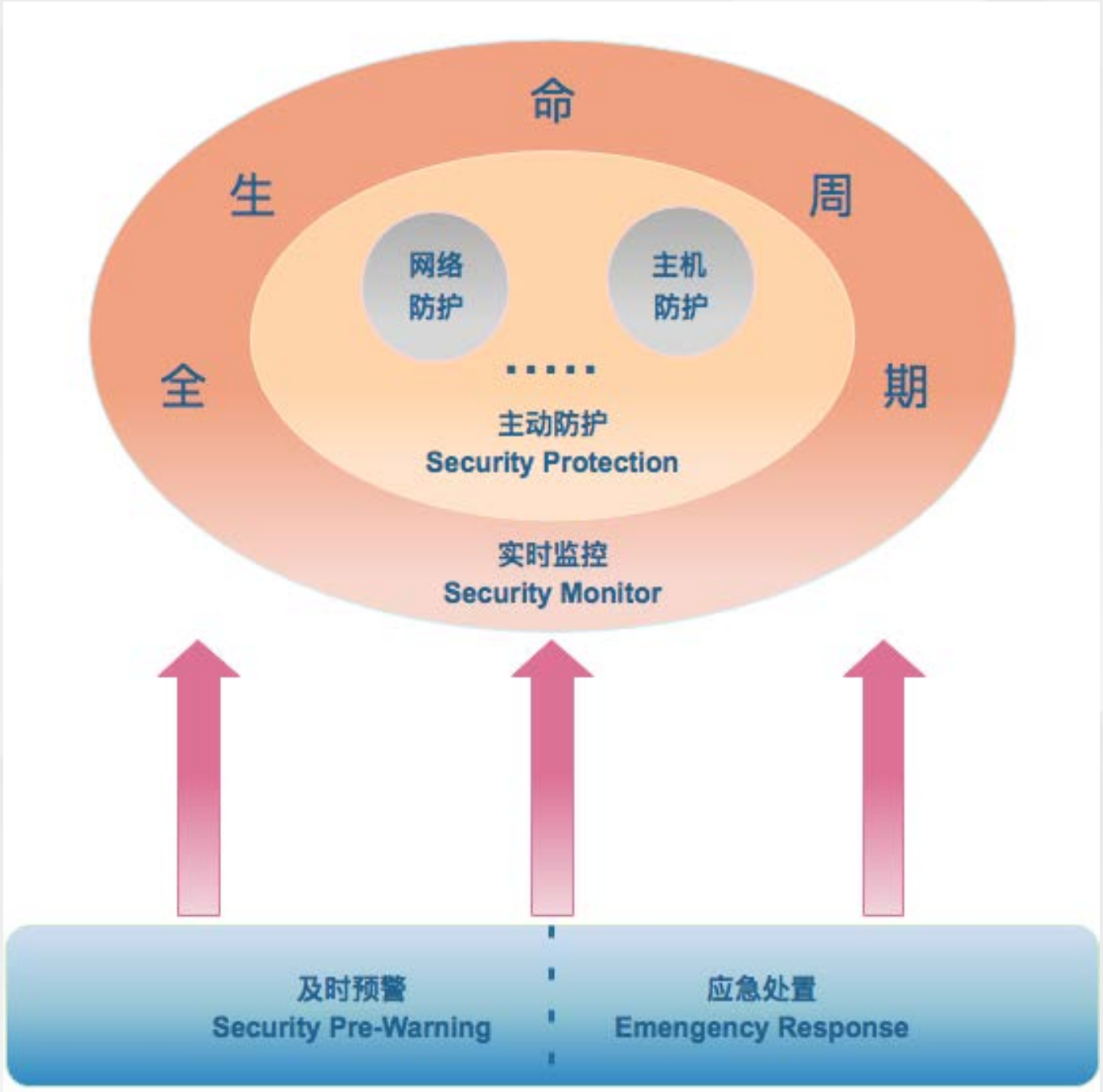
6 关于工控系统安全评估和监管检查

◆关于第三方安全评估或检查：通讯端口、组态开关?

◆多头监管？如何面对?

PART 03

解决方案



PMPE 防护体系

主动防护

安全保障的核心功能，主要包含网络防护和主机等层面。

实时监控

实时监控、管理工业控制系统网络设备和安全设备，全面获取工控网络的安全现状。

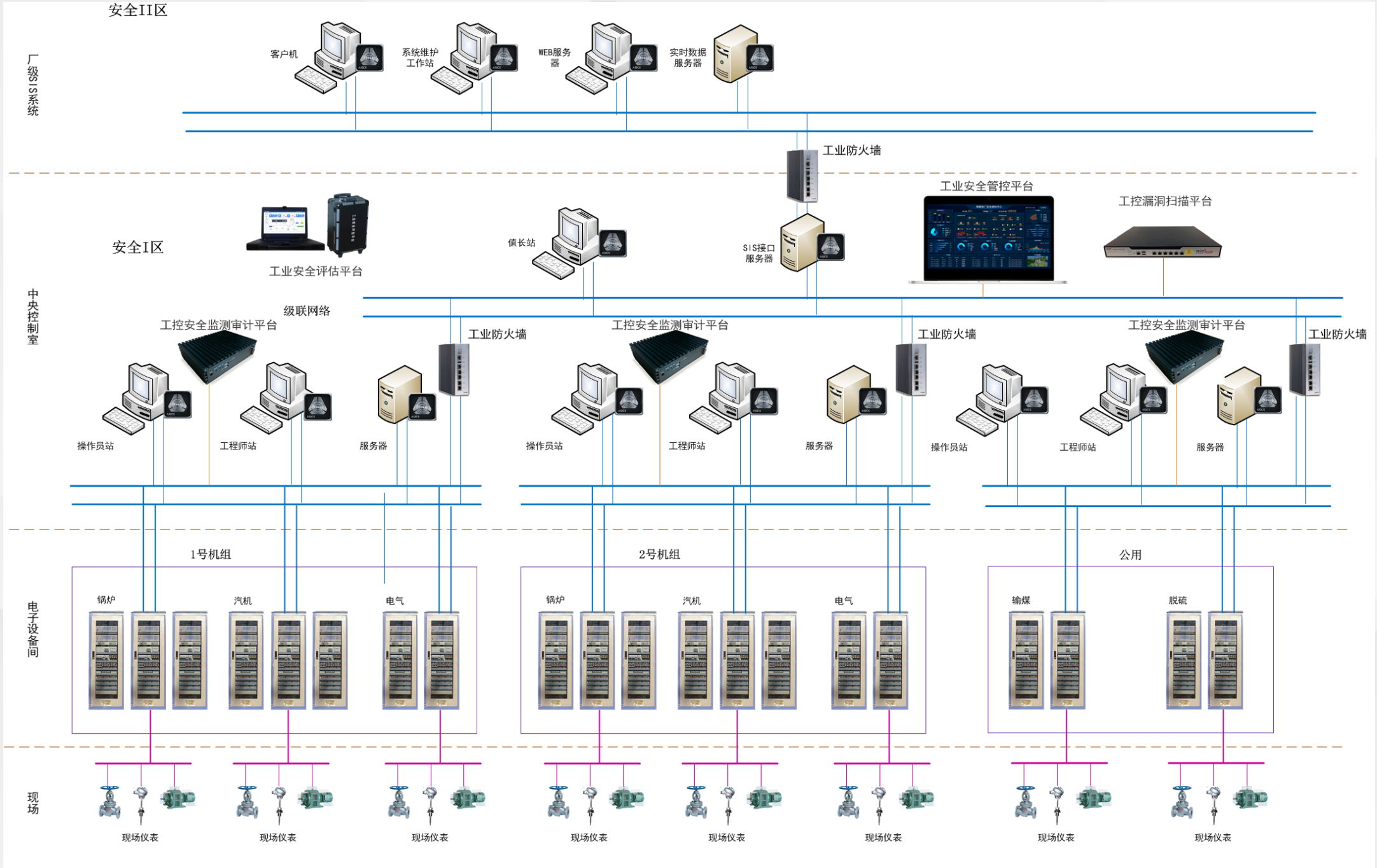
及时预警

定期的安全检查与风险评估，及时有效的漏洞检测，把握工控网络的安全状态。

应急处置

通过平台处置或现场处置，将事故发发生后损失降到最低，最终实现安全防护一体化的目标。

发电厂工控安全原则性网络部署图



关键是做好工控信息安全管理的基础上，

采用技术手段提高热控网络及系统安全水平

打好基础，做好培训

PART 03

研究方向

实时数据库的安全审计

aspentech
Infoplus.21

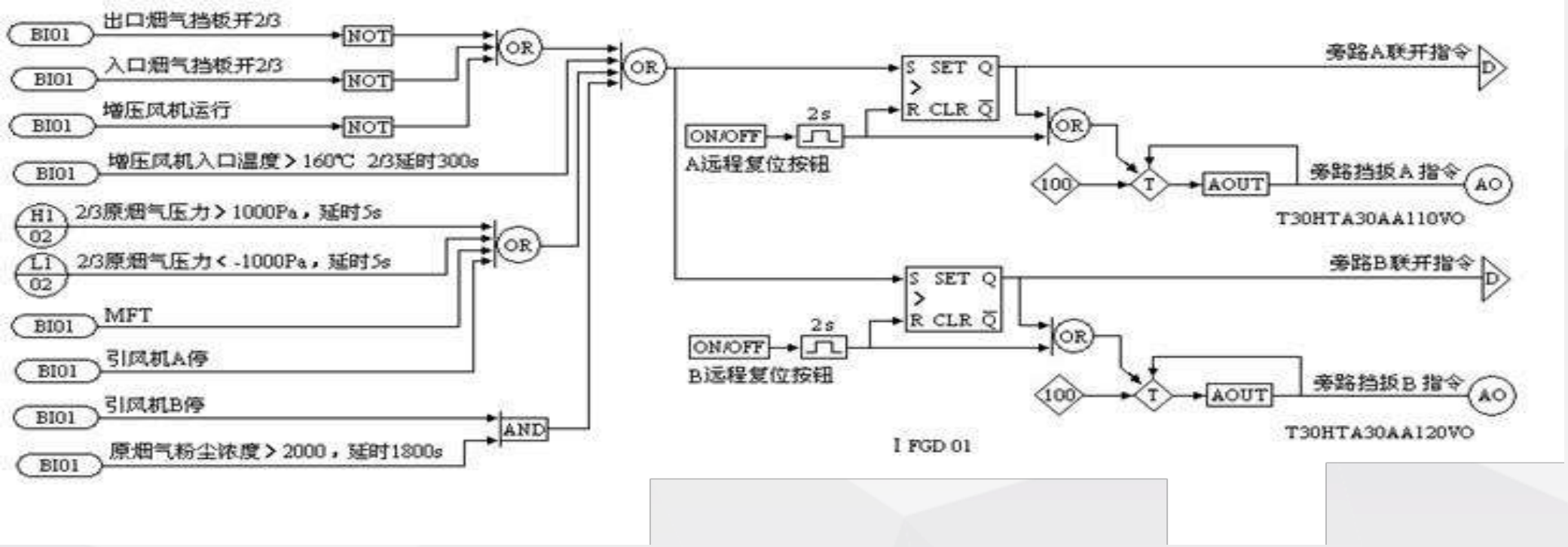
Honeywell
Uniformance、PHD


PI 数据库

三维天地
SuperInfo

	实时数据库	关系数据库
作用	处理实时变化的数据。维护数据的实时性、真实性，满足工业生产管理、实时应用的需要	处理永久、稳定的数据。维护数据的完整性、一致性
读写速度（/ 秒）	1,000,000	3,000
数据恢复功能	无	有
磁盘空间占用率	在单服务器处理30万点，扫描频率为1秒的情况下，实时数据库存贮200小时的数据仅占用4G磁盘空间	同等条件下，关系数据库5小时的数据就达到4G磁盘空间

控制逻辑安全审计



逻辑炸弹，通讯指令、关键指令、重要数据区及符号表、函数调用、甚至组态软件行数。

公司概况

- 国家千人计划获得者创办的高新技术企业
- 国内跻身全球网络安全500强仅有的四家企业之一，是中国领先的专注于信息安全产品和服务的解决方案提供商。
- 业务范围：数据库安全、应用安全、云计算安全、大数据安全、工控安全、以及移动互联网安全、智慧城市安全、智能电厂安全等。
- 员工总数：900多人

谢谢

安恒官微

E安全

钉钉安恒密盾

杭州安恒信息技术有限公司 杜永春 13957152753 yongchun.du@dbappsecurity.com.cn