绿盟工控安全审计系统

产品白皮书

目录

一. 工业控制系统安全概述

1.1 IT 和 OT 的对比

分类	IT	ICS
性能	不需要实时 响应一致 高吞吐量 高的延迟和时基误差可以接受	实时 响应时序要求严格 可接受小的吞吐量 不能接受延迟和时基误差
可用性	重启可接受 有时的不可用是可以接受的，按照系统的运行要求。	由于过程的可用性要求，重启不可接受 冗余设计必须以完成可用性的要求
风险管理	数据的机密性和完整性最重要 容错不是很重要-短暂的停机不是主要威胁。 业务操作的延迟是主要威胁	人们的安全是最重要的，需要保护过程。 容错是重要的，不能短暂宕机。 不合规、环境影响，失去生命、机器和产品是主要的威胁
架构安全	保护 IT 资产和存储在资产和在资产之间交互的信息 中心的服务器需要更多的保护	保护边缘客户端（现场设备等） 保护中心服务器也很重要
无意识的影响	安全解决方案围绕典型的 IT 系统	安全工具必须被测试（线下，在与 ICS 相同的系统中）以保证他们不会影响正常的 ICS 操作
时序严格的交互	紧急情况下的交互不是很重要 为了安全需求，严格的访问控制能够实现	对人操作的响应和紧急情况下的交互非常重要 对 ICS 的访问控制要在不妨害人机交互的前提下进行访问控制
系统操作	系统为了典型的操作系统而设计 更新操作直接用自动部署工具就可以	OS 经常没有内置的安全功能 软件变换要小心。
资源受限	系统有足够的资源来支持第三方的安全解决方案	系统可能没有足够的内存或者计算资源来支持额外的安全能力
通信	标准的通信协议 主要是有线网络，也有一些局部的无线网络 典型的 IT 网络实践	许多转悠的标准通信协议 一些类型的通信媒介，如专用的有线和无线（无线电通信和卫星通讯） 网络很复杂，需要调度工程师专门的知识
变更管理	当有好的安全策略和过程出现	软件的改变必须经过完全的测试，递增

	时，软件会及时改变，过程通常是自动的。	的部署到系统中，保证系统的完整性。ICS 中断供应必须提前几天或者几个星期计划，ICS 可能会使用不再被生产生提供支持的 OS 系统。
管理支持	提供多样化的支持	通常只有一个供应商
部件的生命周期	3-5 年	15-20 年
部件的访问控制管理	部件在本地，容易访问	部件可能是隔离的、分布在远端的，并且需要大量的体力访问他们。

1.2 保护工业控制系统安全的 7 个策略

（1） 实现应用白名单（Application Whitelisting , AWL）

（2） 确保合适的配置和补丁管理

（3） 减少攻击面

（4） 建立一个可防御的环境

（5） 管理认证

（6） 实现安全的远程访问

（7） 监测和响应

以上 7 个步骤涉及到了很多的安全产品，例如：

市场上已经出现了多款主机白名单产品，解决了工控系统主机病毒感染、恶意脚本执行、操作系统内核漏洞隐患、应用程序缓冲区溢出攻击等问题，实现了主机保护。绿盟工控漏洞扫描系统可以对一些关键系统的安全配置进行评估，进行配置管理。使用 IDS、防火墙产品在

边界上对 ICS 进行防护。还有一些可信网关、工业异常检测、安全审计等产品，可以用于实现以上的 7 个策略。

虽然这个策略可以防止 90%多的攻击，但是还有剩下的一些攻击手段，需要持续性的监测。此外，对于一些严重程度较低的异常，有些安全管理员很可能会忽略这些警告，而这很可能是有敌手对工控系统进行 APT 攻击，如果将这些异常信息进行关联分析，从中发现潜在的安全隐患，不仅能够减少管理员的压力，同时还能更好地保护工控安全。

在第七个策略安全监测和响应中，需要对位于现场控制层的控制设备以及位于过程监控层的工作站的通讯过程进行安全监控。由此，可将工控安全监测预警体系的创建分为三个步骤。

（1）根据上文提到的 7 个策略，在工控各个节点添加适用于工控的安全设备，如在边界防护方面，布置工控防火墙、IDS 等。对工控网络内部，使用工控异常行为监测系统、资产识别系统等。将这些底层的安全系统部署在工控环境中，就可以很大程度地提升工控系统的安全性。

（2）众多的底层安全系统之上，我们还需要一个监测审计和分析系统，来对各个底层设备产生的告警记录、日志进行汇总、精炼和关联分析，深入挖掘出这些记录之中隐藏的信息。对工控系统整体的安全态势有了了解。

（3）对未来的安全态势做出预测，如果可能提供必要的安全措施的建议，同时提供更友好的可视化技术。

经过分析我们发现，现在的工控网络安全监测预警方案的建立仍然处于第一阶段，我们需要根据工控安全需求和脆弱性，结合 7 个策略，制定适用于工控的安全产品，从各个威胁点上保护工控环境的安全。在众多工控安全系统中，工控网络异常监测系统是搭建整个预警体系的关键所在。作为预警体系的探针，工控网络异常监测系统承载着数据收集和分析的要务。

适用于工控网络的异常监测系统，需要对对手的入侵主动监测，快速执行已经准备好的响应方案。

可考虑在五个位置部署监控程序：

1） ICS 边界对 IP 流量进行监测，正常和非正常的通信

2） 在控制网络中的 IP 流量，恶意的连接或者内容

3） 基于主机的产品，监测恶意软件和攻击企图

4） 登录分析（时间或者地点），监测被盗用的账号的使用或者不正确的访问，验证所有的异常现象，通过快速电话联系。

5） 监测用户的管理行动，检测访问控制操作。

二. 绿盟工控安全审计系统

2.1 概述

当前工控系统安全保障正面临五大挑战：一是安全失衡，即重发展、轻网络，重功能安全、轻信息安全；二是态势失察，即资产底数不清、安全态势不明、风险预警缺乏；三是诊断失据，即审查评估无标准、安全防护无指南、测试工具不成熟、诊断环境受限制；四是防护失效，由于工控系统的特殊性，导致大量现有的信息安全措施无法直接应用于工控安全防护工作中；五是力量失衡，由于我国工控安全研究力量分散，仍无专注于工控安全的先进的、权威的技术研究与支撑机构，以至于目前对工控安全的态势感知、有效防控、应急恢复、预测分析技术的保障能力还处于初级水平。基于以上安全现状，我司针对工控系统可能发生的异常行为进行安全监测研究，深入解析不同行业工控系统使用的工控协议，重点研发了新版本的工控安全审计系统。

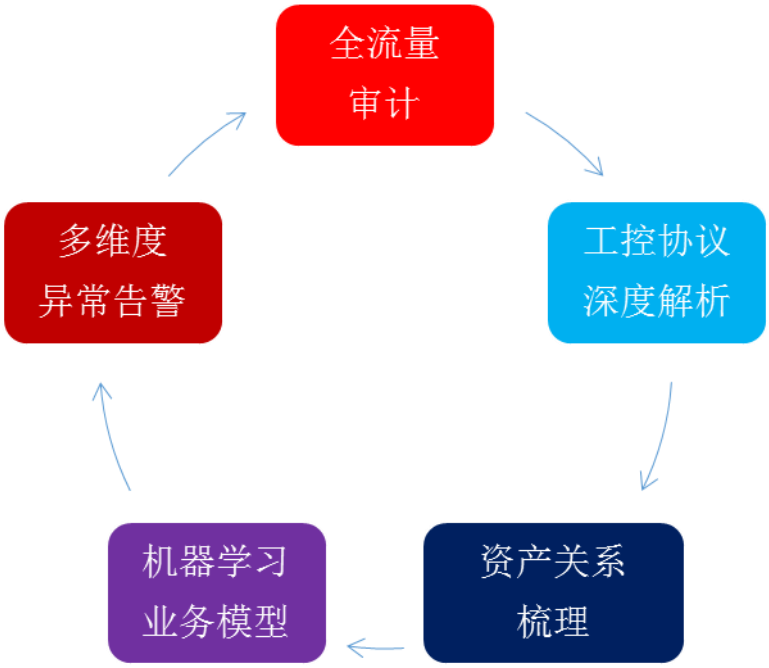

图 2.1 绿盟工控安全审计系统产品功能导图

绿盟工控安全审计系统，是专门针对工业控制网络的安全审计系统。不仅包括网络安全层面的异常监测，还融入了不同行业的业务安全告警，如智能变电站场景下的遥控操作、定

值切区操作、定值修改操作等关键业务行为告警。工控安全审计系统采用旁路部署模式，对工业生产过程“零风险”，基于对工业控制协议（如 Modbus TCP、 OPC、Siemens S7、DNP3、IEC 60870-5-104、IEC 61850-MMS、IEC 61850-GOOSE、IEC 61850-SV 等）的通信报文进行深度解析（DPI，Deep Packet Inspection），能够实时检测针对工业协议的网络攻击、用户误操作、用户违规操作、非法设备接入以及蠕虫、病毒等恶意软件的传播并实时报警，同时详实记录一切网络通信行为，包括指令级的工业控制协议通信记录，为工业控制系统的安全事故调查提供坚实的基础。

绿盟工控安全审计系统，可广泛应用于电力、石油、石化、轨道交通、烟草、煤炭、钢铁及先进制造等各个行业。

2.2 产品架构

NSFOCUS SAS-ICS 主要由基础服务层、数采分析层、核心业务层、用户接口层共四个部分组成，可以在各种不同场景的工业网络环境中进行灵活的部署和管理，如图 2-1：

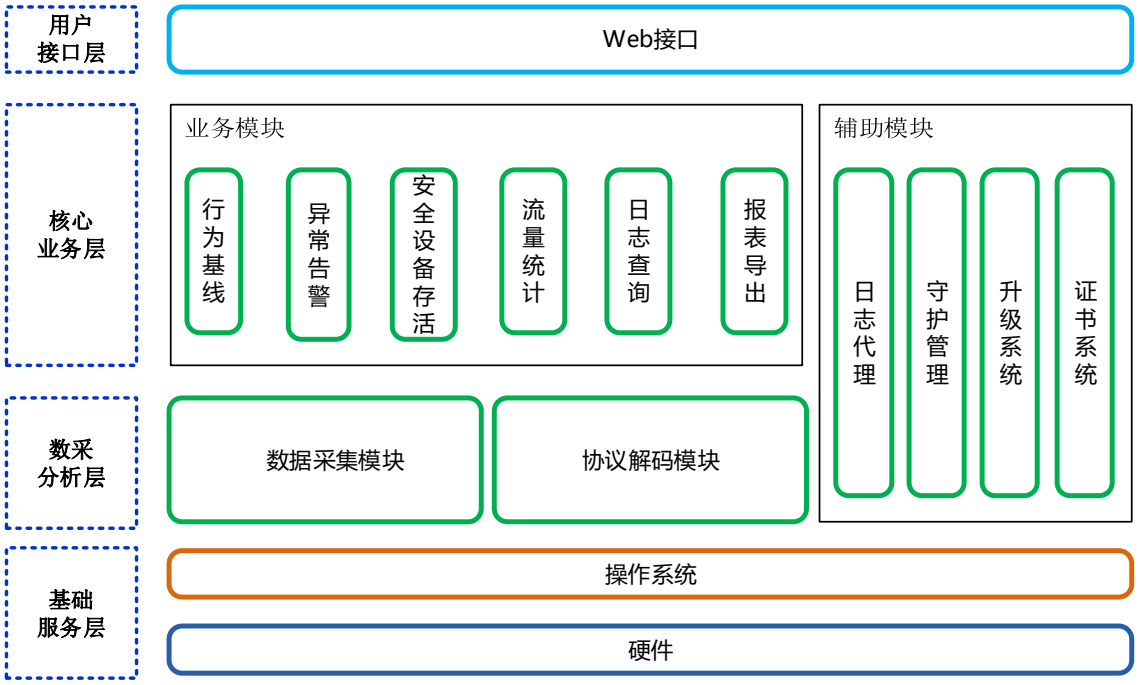

图 2.2 绿盟工控安全审计系统架构图

① 基础服务层

使用专用的硬件平台，提供可靠稳定的硬件环境，辅助以系统运行的必须软件，组成基础平台层，支持传统 IT 网络协议，支持工业网络协议。

② 数据分析层

主要是数据采集模块和协议解码模块，对工控协议进行深度解析和分析，提取关键操作行为。

③ 核心业务层

在该层实现系统的应用功能的实现。包括基于工控场景的业务行为基线，基于黑白名单的异常行为告警。

④ 用户接口层

在该层实现和最终用户的人机界面，通过 WEB 接口进入管理界面进行系统配置管理。

三. 绿盟工控安全审计系统产品特性

3.1 基于机器自学习的业务行为基线

工业网络中设备众多、网络通信复杂，用户很难全面的掌握网络中所必须的业务通信需求，这会给安全设备的规则配置带来很大的困难。为了方便用户进行异常行为检测规则的配置，提高规则配置的准确性，减少规则配置的工作量，NSFOCUS SAS-ICS 开发了基于机器自学习的业务行为基线功能。该功能采用被动检测的方式从网络中采集数据包，并进行数据包的解析，智能的与系统内置的协议特征、设备对象等进行匹配，生成可供参考的网络交互信息列表，通过对协议分布和流量信息的匹配，形成“工控场景行为基线”，帮助用户以最直观的方式了解和掌握网络中的业务通信状态，发现工控网络潜在的安全风险。

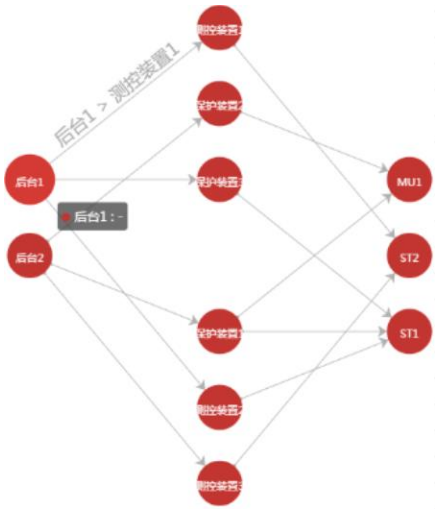

图 3.1 工控网络基线资产关系图

通过基线自学习功能梳理工控现场资产拓扑，建立工控网络行为模型，对基线外异行为如组态变更、操控指令变更、负载变更、异常访问等告警，实现对工控现场安全事件的告警与响应，保障工业控制系统的安全稳定运行。

3.2 深度融合业务场景的异常行为检测

电力、石油、石化、轨道交通、烟草、煤炭、钢铁及先进制造等各个行业的工业控制系统千差万别，不同的工艺流程往往有着不尽相同的业务处理方式，针对不同行业工控网络的异常监测有着较强的特异性差异。NSFOCUS SAS-ICS 深入不同行业的 OT 网络场景，融入针对不同行业的业务安全告警。如针对变电站场景，可对 IEC 61850 协议簇进行深度解析，对应到特定场景下的关键操作行为（遥控操作，改定值操作）；针对其他行业场景，可设置通用行业场景，解析 Modbus TCP、S7 Comm 等常见协议规约。

同时，NSFOCUS SAS-ICS 可对工控系统的配置文件进行解析，如变电站 SCD 文件等厂商相关配置文件的解析，将功能代码与具体业务操作进行关联，实现业务安全审计的功能。如可对工控协议报文进行检测和告警。可对运维人员下发的工控协议报文产生的非法操作进行检测和告警。可对资产新增、路径异常、未知协议、越权操作、关键控制等行为进行检测和告警。

3.3 工业网络协议深度解析

绿盟科技基于对工控环境的理解，针对工控环境使用的规约进行了相关的分析和研究，对于协议的内容进行了完全的解码，可以深入到指令级别的分析，对于从上位机指令下发控制端到下位机指令接受操控端的通讯过程进行全面细致的解析。如对 Modbus Tcp 协议，可以深入到功能码寄存器层面进行细致的监测审计（写多个寄存器、读保持寄存器等）。

编号	功能码
1	read coils
2	read input discretes
3	read mult regs
4	read input regs
5	write coil
6	write single reg
7	read except stat
8	diagnostics
9	get comm event ctrs
10	get comm event log
11	write mult coils
12	write mult regs
13	report slave id
14	read file record

图 3.2 深入到功能码寄存器层面的工控协议深度解析

NSFOCUS SAS-ICS 通过镜像方式对流量进行深入解码，分析其中的操作是否符合定义的操作要求，如发现其中有任何的违规操作，及时进行报警，由管理员来进行相关的处理。

3.4 工业控制系统行业场景网络拓扑

在部分工业控制系统环境中，由于系统使用者和系统管理者很有可能分属于两个部门，所以没有相关人员对工业控制系统进行过资产的梳理，拓扑的更新等操作，并且由于工控设备大多数部署在工控现场，可能位于不同机柜甚至位于不同的地区，在进行工业控制系统资产梳理和拓扑编制的过程中存在较多困难点。

针对此种情况，绿盟工控安全审计系统以资产管理为导向，预制了不同工业环境下的工业网络分层拓扑结构图，展示被监听的工业网络场景下的网络资产。

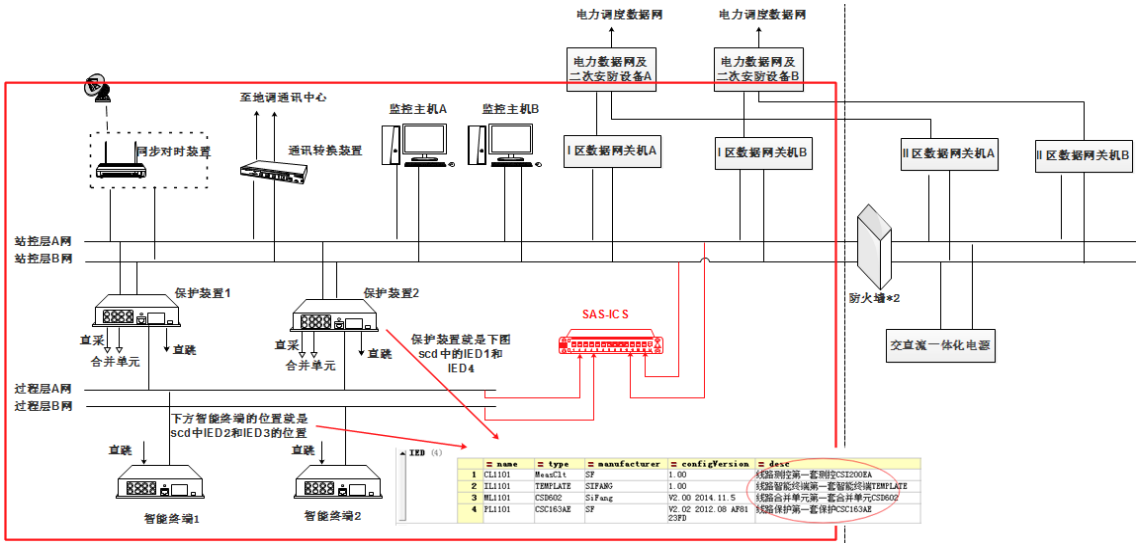

图 3.3 工业控制网络行业场景拓扑图

3.5 覆盖多种行业的工控协议识别

NSFOCUS SAS-ICS 的安全监测审计行为对工业生产过程“零风险”无扰动，基于对多种行业的工业控制协议（如 Modbus TCP、COTP、OPC、Siemens S7、DNP3、IEC 60870-5-104、IEC 61850-MMS、IEC 61850-GOOSE、IEC 61850-SV 等）的通信报文进行深度解析（DPI，Deep Packet Inspection），能够实时检测针对工业协议的网络攻击、用户误操作、用户违规操作、非法设备接入以及蠕虫、病毒等恶意软件的传播并实时报警，同时详实记录一切网络通信行为，包括指令级的工业控制协议通信记录，为工业控制系统的安全事故调查提供坚实的基础。

3.6 传统 IT 网络行为审计

NSFOCUS SAS-ICS 支持对传统 IT 网络环境使用的 HTTP、FTP 等协议的文件传输进行审计，支持对 TELNET、FTP 等业务操作进行命令级审计。可基于 IP 地址、用户/用户组、时间、关键字等多种组合审计策略。

3.7 高可靠的自身安全性

产品本身采用独立的硬件平台，数据分区加密，Web 站点访问采用 HTTPS 方式访问；产品本身屏蔽关键扫描服务外的其他服务端口；产品涉及用户更密码的地方都加密处理，保证密码的安全性；产品相关任务，日志，数据等导出都采用独立的加密处理；产品升级及证书系统采用高等的数据加密处理；提供独立的产品诊断 Consle，保证系统的可维护性。

3.8 多样化部署模式

NSFOCUS SAS-ICS 采用旁路部署，通过流量镜像的方式对工控网络进行全流量数据监听，不主动发包，对工控系统“无扰动，零风险”，不做网络的任何修改；可覆盖 DCS 网络、PLC 网络、数控机床 DNC 网络等不同行业应用场景的工控系统。

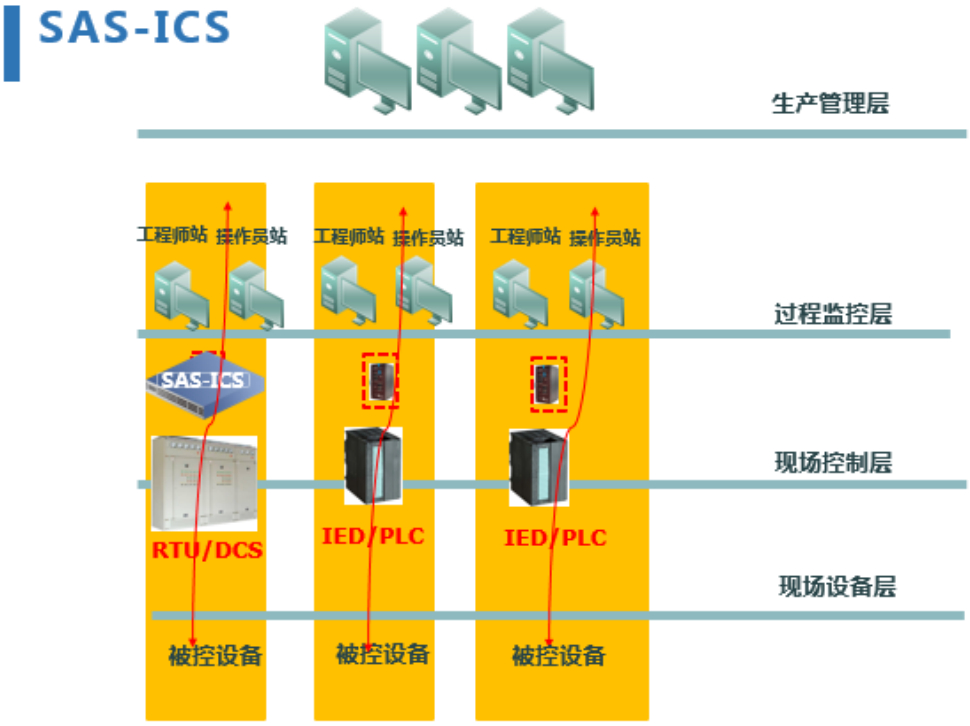

图 3.4 绿盟工控安全审计系统典型部署方式

四. 结语

由于工业控制系统所覆盖的行业重要性，比如油化、电力、核电厂、水利、交通、市政、军事、高端制造业等，其安全性问题也越发的重要，并且牵涉到国计民生。对于这些关键信息基础设施，如何进行安全监测及预警，如何及时有效的进行事前的防范，事中的监测以及事后的追溯，正成为工控安全领域亟待解决的问题。

NSFOCUS SAS-ICS 能够像“黑匣子”一样精准记录工业控制系统内部的网络通信行为，为可能出现的安全隐患提供详实的记录。可以对工业网络出现的网络异常行为、针对工业协议进行的不合规攻击以及工业控制流程出现的关键操作进行实时的检测与告警。业界独创的基于机器自学习方法的业务行为基线功能可适用于多种复杂工业控制系统，帮助现场用户快速定位和解决安全问题。

五. 附录

参考文献：

① [工信部]《工业控制系统信息安全防护指南》

② [工信部]《工业控制系统信息安全事件应急管理工作指南》

③ [工信部 451] 关于加强工业控制系统信息安全管理的通知，工信部协[2011]451 号

④ [国能安全 36 号文]《关于印发电力监控系统安全防护总体方案等安全防护方案和评估规范的通知》

⑤ [发改委] 第 14 号令《电力监控系统安全防护规定》

⑥ [电监会 2013] 电监会 2013 年 50 号文，《电力工控信息安全专项监管工作方案》

⑦ [国家能源局,2013] 国家能源局国家能源局关于近期重点专项监管工作的通知（国能监管〔2013〕432 号）

⑧ [绿盟科技]《2015 绿盟工控安保框架白皮书》

⑨ [Gartner] Gartner 《Definition: Operational Technology Security 2013》

⑩ CONTROL ENGINEERING ® China 2014.3 《如何实现以太网的快速迁移》