工业控制系统信息安全产业联盟
ICSISIA

从乌克兰和委内瑞拉电网事件谈“工控系统网络安全保护”

冯冬芹

浙江大学 工业控制系统安全技术国家工程实验室
网控空间网络安全教育部重点实验室
IEC/TC65/WG20,WG10(IEC62443);ISA/ISA99

一、事件回顾

二、一些思考

三、一点建议

乌克兰大规模停电事件（2015）

- 2015年12月23日当地时间15时左右，乌克兰首都基辅部分地区和乌克兰西部的 140万名居民突然遭遇了一次长达数小时的大规模停电，至少三个电力区域被攻击。
- Kyivoblenergo电力公司称：公司因遭到入侵，导致7个110KV的变电站和23个35KV的变电站出现故障，导致 80000用户断电。

12/24/2015

Dear customers!

Dec. 23, 2015, from 15:35 - 16:30, third parties were made illegal entry into information-technological system of remote access to equipment telecontrol substations of 35-110 kV JSC "Kyivoblenergo."

As a result, it was disconnected 7 (seven) 110 kV substations and 23 (twenty three) substation 35 kV. This led to the repayment of about 80,000 different categories of customers on the reliability of electricity supply.

Electricity was restored to all consumers employees of the Company at **18:56** the same day.

We apologize for the situation and thank you for your understanding.

PJSC "Kyivoblenergo"

ww.winicssec.com/Index/show/catid/57/id/347.html

乌克兰电力部门感染BlackEnergy

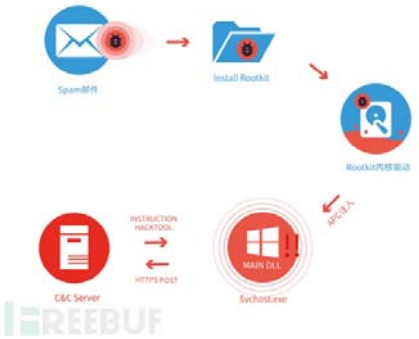
① 黑客通过收集目标用户邮箱，然后向其定向发送携带恶意文件的Spam邮件

② 疏于安全防范的用户打开了带宏病毒的Office文档（或利用Office漏洞的文档）即可运行Installer（恶意安装程序），Installer则会释放并加载Rootkit内核驱动

③ Rootkit使用APC线程注入系统关键进程svchost.exe（注入体main.dll）

④ main.dll会开启本地网络端口，使用HTTPS协议主动连接外网主控服务器

⑤ 一旦连接成功，开始等待黑客下发指令就可以下载其他黑客工具或插件。



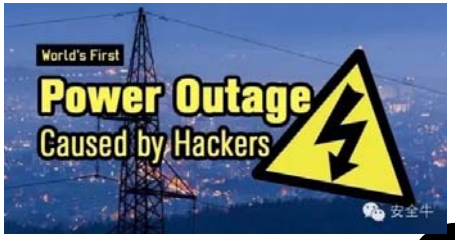
https://www.freebuf.com/articles/network/93092.html

BlackEnergy典型组件

1	Msiexec.exe	一个Installer,管理软件的安装、软件组件的添加和删除，监视文件复原、灾难恢复等。
2	reDuh	HTTP隧道传输TCP的工具，用于从外部访问内网
3	weevely3	命令行的webshell，同样用于外网访问内网
4	dropbear	重新打包的SSH服务器，内置了硬编码的口令
5	DSEFix	下载未签名驱动绕过系统保护的工具
6	KillDisk	现场破坏工具，对MBR（Main Boot Record）写操作，破坏计算机

http://www.winicssec.com/Index/show/catid/57/id/347.html

BlackEnergy攻击步骤



1 对SCADA界面篡改，蒙蔽现场调度人员

2 大量电话DoS攻击基辅电力呼叫中心，使之无法响应用户申诉

3 用Killdisk组件擦除关键数据，拖延恢复时间，并使得事后取证更加困难

4 感染控制工作站，开启断路器

哪个组件？
如何做到？

乌克兰第二次停电事件（2016）

- 2016年12月17日当地时间23点多，乌克兰的国家电力部门又一次遭遇了黑客袭击，这次停电持续了 30 分钟左右，受影响的区域是乌克兰首都基辅北部及其周边地区。
- 30分钟后，Ukrenergo工程师将设备切换为手工模式，并开始恢复供电，75分钟后完全恢复供电。

http://www.winicssec.com/Index/show/catid/57/id/347.html

CrashOverride（Industroyer）

◆2017年6月12日，美国安全厂商 ESET 公布一款针对电力变电站系统进行恶意攻击的工控网络攻击武器 -win32/Industroyer（ESET命名），ESET 表示该攻击武器可以直接控制断路器，可导致变电站断电。

◆ Industroyer 恶意软件目前支持四种工控协议：IEC 60870-5-101、IEC 60870-5-104、IEC 61850以及OLE for Process Control Data Access（简称OPC DA）。

◆与2015年袭击乌克兰电网最终导致2015年12月23日断电的攻击者使用的工具集（BlackEnergy、KillDisk、以及其他攻击模块）相比，这款恶意软件的功能意义重大，它可以直接控制开关和断路器，无需所谓的漏洞

https://paper.seebug.org/328/

Industroyer 思路

① ◆首先黑客可以通过电子邮件、办公网系统、外来运维终端、U盘等途径成功入侵一台主机(如：内网的10.15.1.69)，并且在该主机联网时下载必要的模块，执行比如 Tor 网络客户端或者代理服务模块等作为后续攻击的回连跳板

② ◆接下来以该主机为跳板对系统局域网络进行探测扫描，当发现自己感兴趣的目标(是否为104从站、OPC服务器或者操作站等)后对其实施攻击

③ ◆一旦攻击成功，黑客就将这台可以连接外网的主机 IP 配置为攻击模块 Main Backdoor 的代理IP，下发到该主机中，这台主机是可以直接与 RTUs 或者 PLCs 进行通信的，并且可以做直接的控制。

Industroyer 组件

（1）一个主后门模块Mainbackdoor：用于连接C&C下载另外一批功能模块执行

（2）一批功能模块：

① 实现 DLL Payload 模块执行的加载器模块

② 实现数据及痕迹清理的 haslo 模块

③ 实现IP端口扫描的 port 模块

④ 实现西门子 SIPROTEC 设备 DoS 攻击的 DoS 攻击模块

（3）其中，DLL Payload 模块包含：

① 实现 IEC 101 工控协议的 101.dll 模块

② 现 IEC 104 工控协议的 104.dll 模块

③ 实现 IEC 61850 协议的 61850.dll/61850.exe 模块

④ 实现 OPC DA 协议的 OPC.exe/ OPCClientDemo.dll 模块等

https://paper.seebug.org/328/

载荷组件的技术原理与细节？

委内瑞拉停电事件（2018）

- 2019年3月7日傍晚（当地时间）开始，委内瑞拉国内包括首都加拉加斯在内的大部分地区停电超过24小时，在委内瑞拉23个州中，一度有20个州全面停电
- 停电导致加拉加斯地铁无法运行，造成大规模交通拥堵，学校、医院、工厂、机场等都受到严重影响，手机和网络也无法正常使用。
- 8日凌晨，加拉加斯部分地区开始恢复供电，随后其他地区电力供应也逐步恢复，但是9日中午、10日的再次停电，给人们带来巨大恐慌。

https://www.freebuf.com/articles/paper/198406.html

委内瑞拉停电事件（2018）

◆初次停电是因为南部玻利瓦尔州的一座主要水电站发生故障，属于古里（Embalse de Guri）水电站，年发电量约为47,000GWh,约占委内瑞拉用电量的近四成

◆3月11日晚，马杜罗表示电力系统遭遇了三阶段攻击。

① 第一阶段是发动网络攻击，主要针对西蒙·玻利瓦尔水电站，即国家电力公司（CORPOELEC）位于玻利瓦尔州（南部）古里水电站的计算机系统中枢，以及连接到加拉加斯（首都）控制中枢发动网络攻击

② 第二阶段是发动电磁攻击，“通过移动设备中断和逆转恢复过程”

③ 第三阶段是“通过燃烧和爆炸”对Alto Prado变电站（米兰达州）进行破坏，进一步瘫痪了加拉加斯的所有电力

◆3月12日，马杜罗在一次电视直播的活动中再次透露，攻击是在五角大楼的命令下由美军南方司令部直接执行的。同时，马杜罗请求俄罗斯、中国、伊朗和古巴协助

https://www.freebuf.com/art...1984(

委内瑞拉水电站发生了何种故障？为什么不能短时间恢复？

一、事件回顾

二、一些思考

三、一点建议

为什么是电力系统?

一类:国家重大武器装备

二类:国家关键基础设施。可能导致国民经济混乱。
如电网、重大水利、核电、枢纽油气管线、大型炼油厂、机场等

三类:国家重要基础设施。可能导致环境破坏和社会动荡。
如自来水、城市交通、含有有害化学物质的化工厂

四类:其他重要设施。可能造成环境破坏、伤亡和经济损失。
如工业企业、医疗设施、一般化工厂、近居民区的加油站等

针对工控系统的攻击组成有哪些？

针对工控系统的（精准）操控与欺骗

计算机、互联网漏洞利用

载荷部分（常规、核）

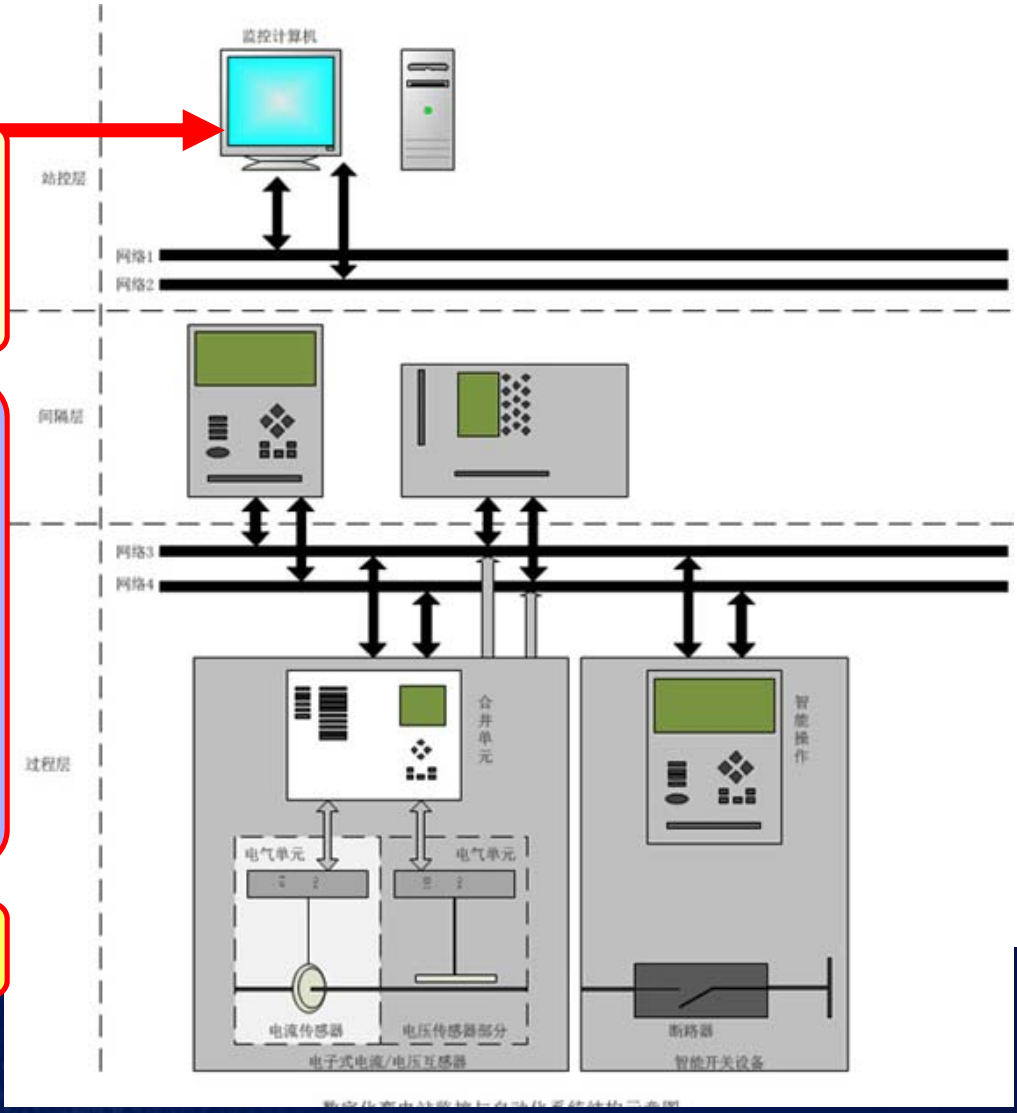
运载部分

运载部分对工控系统的威胁

- 传统计算机安全、互联网安全威胁
  - 工程师站、操作员站的电脑
  - 操作系统、 TCP/IP、软件

- 获取计算机（工程师站、操作员站）电脑权限
- 运载针对工控系统的有效载荷
- 窃取文件、破坏文件、锁住文件与软件（如WannaCry）、导致黑（蓝）屏、等
- **但对生产的核心控制与运行影响有限，**如2017年中石油加油站受WannaCry攻击，加油功能正常，支付功能受影响

- 特点：非法操作、显性破坏、易被发现

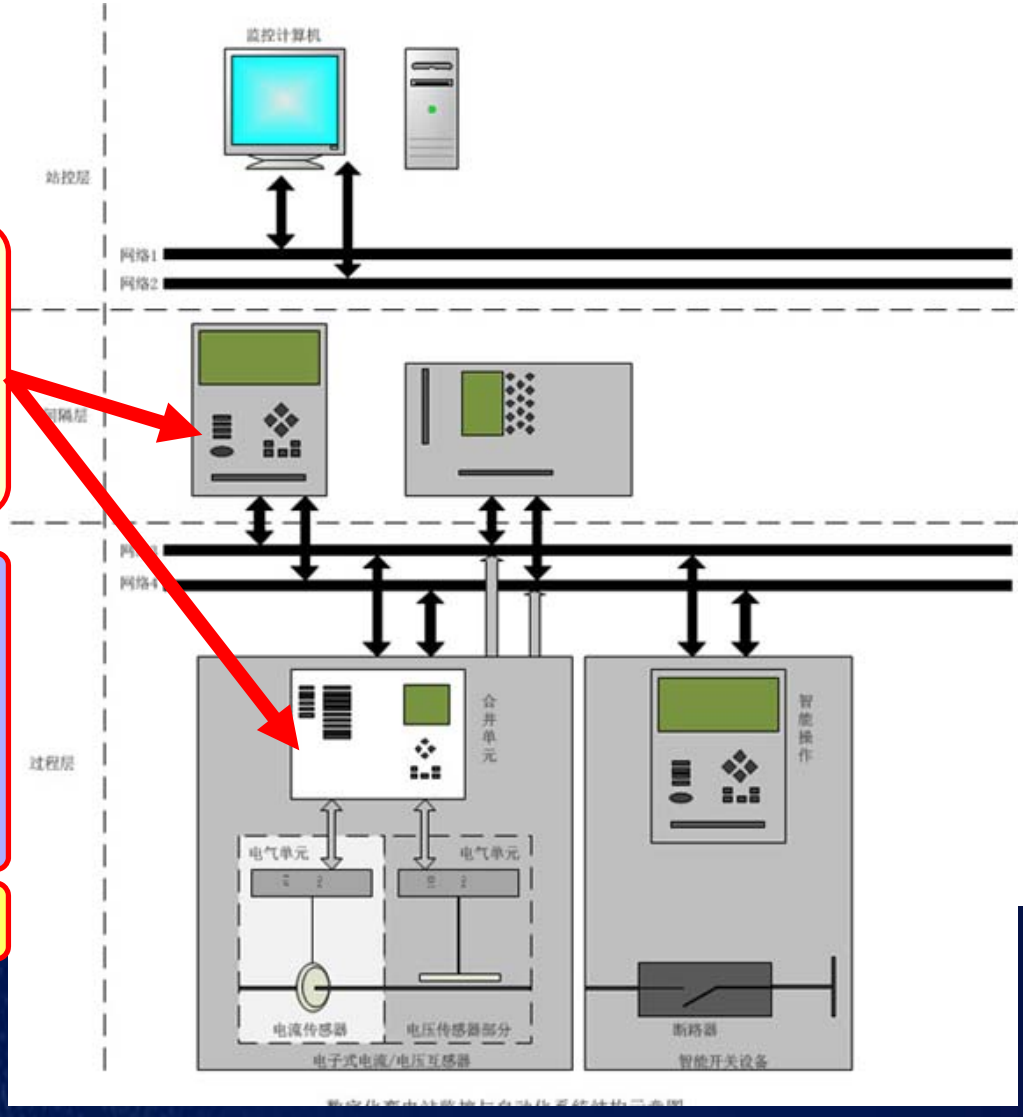


载荷部分对工控系统的威胁

- 工控系统（核心部件）安全威胁
  - 嵌入式控制站（如DCS控制站、PLC设备等）
  - 中低速现场总线（如Profibus）
  - 现场智能仪表（传感器、变送器、执行机构等）

- 利用PCS7控制系统本身的“合法”协议、“合法”指令、“合法”数据
- 恶意代码的注入、所发出的恶意操控指令、虚假的“正常”生产工况数据
- 如Industroyer据传“没利用”任何工控漏洞

- 特点：利用合法协议与指令，不易发现，隐蔽性强



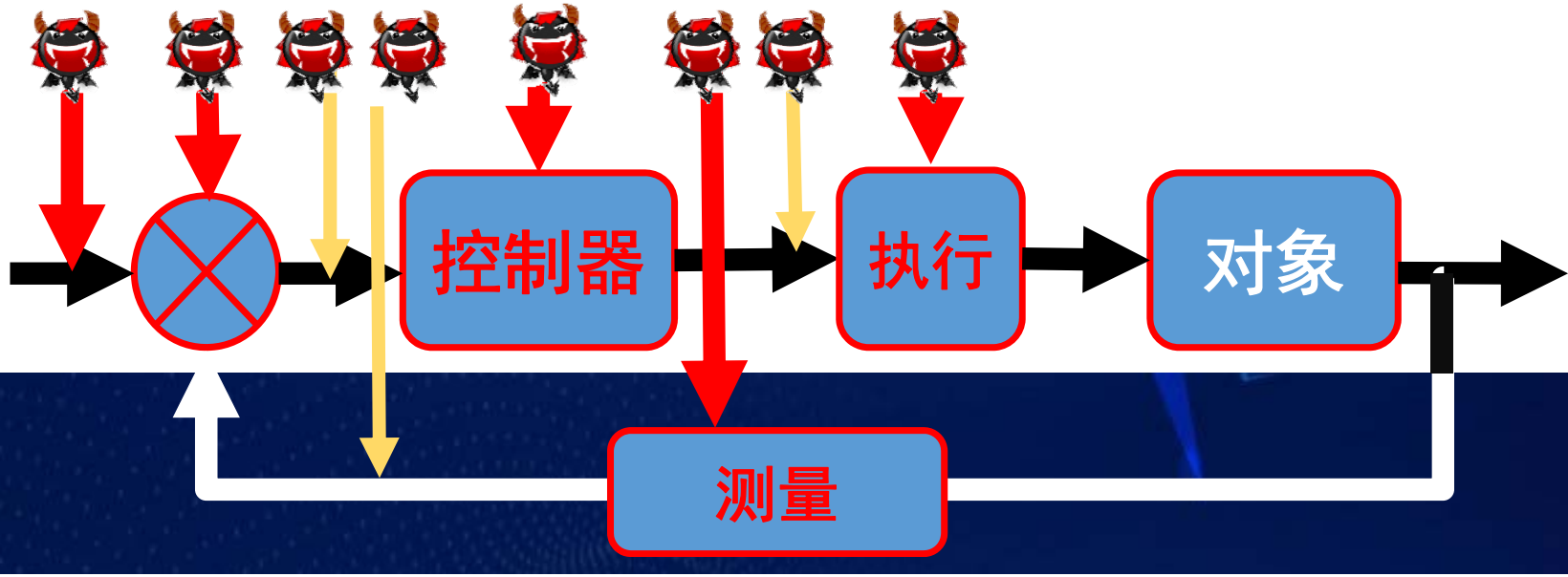
载荷部分对工控系统的攻击形式

信道攻击

- 干扰通信
- 消耗资源
- 修改参数

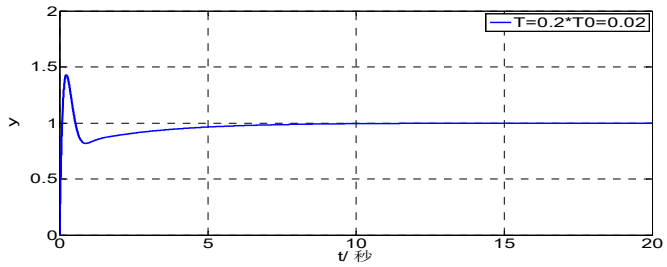
代码攻击

- 控制器、I/O
- 恶意指令、操作数据
- 实时数据欺骗



攻击类型

干扰型攻击（丢包、干扰）

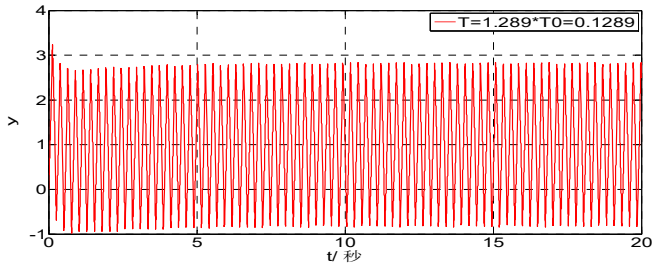


正常：

工控系统一般具有一定的稳定性能力

产品质量变差

操控型攻击（精准）



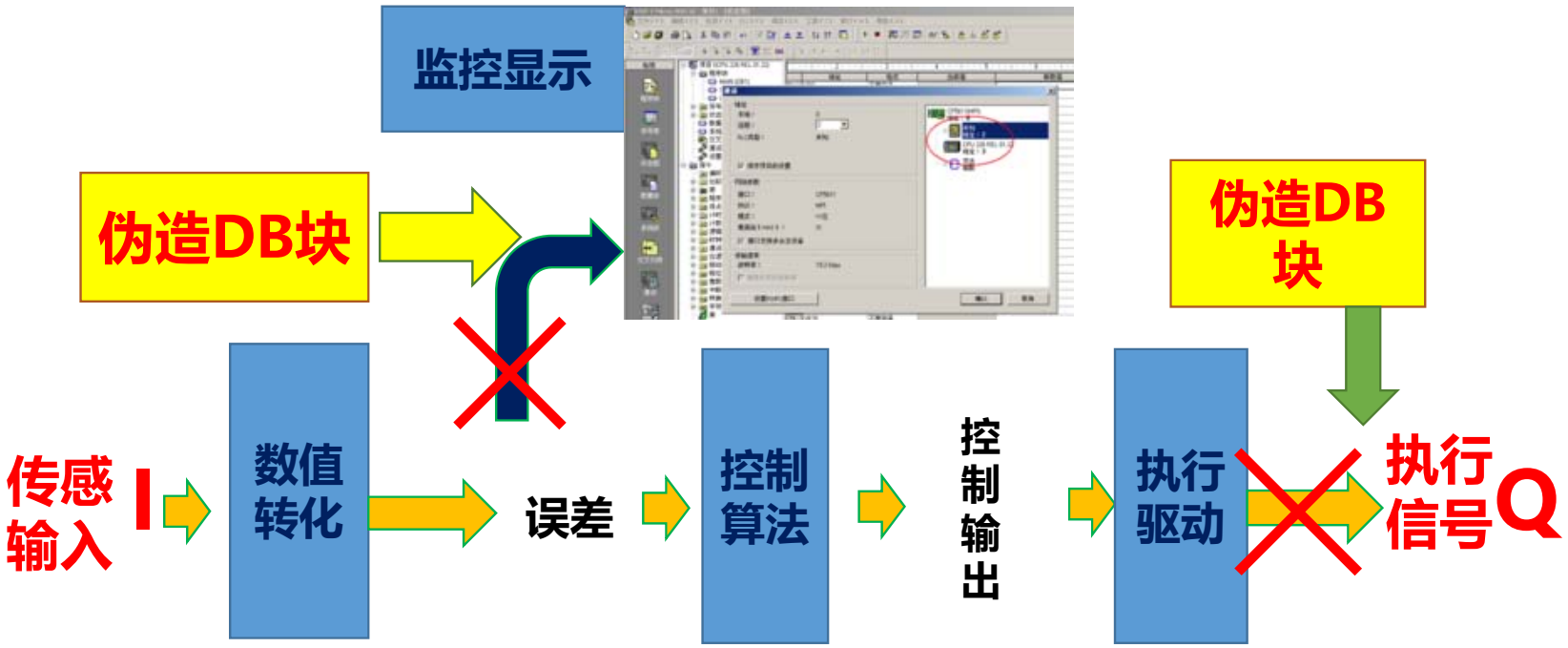
异常：

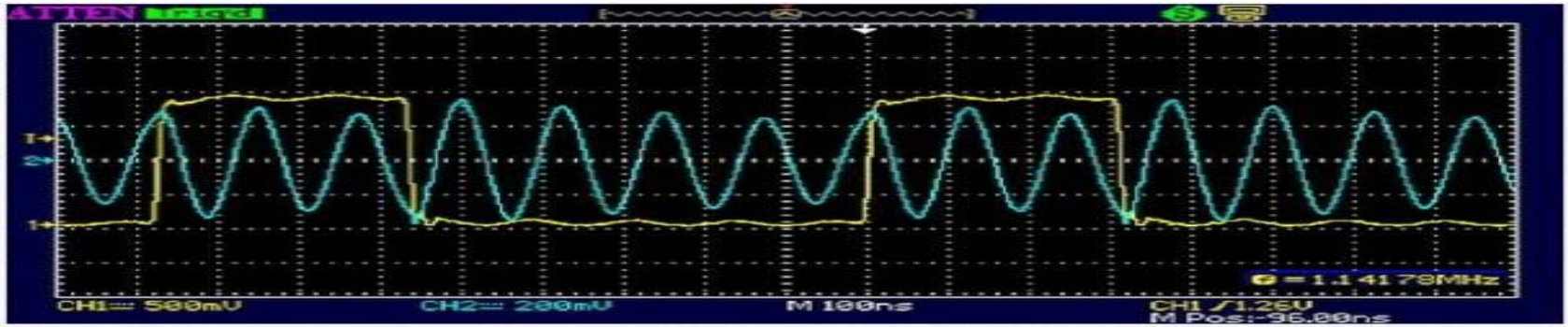
致不稳定、破坏平衡（引发破坏、事故）

生产线停产

灾难事故

精准攻击形式：恶意操控，实时欺骗



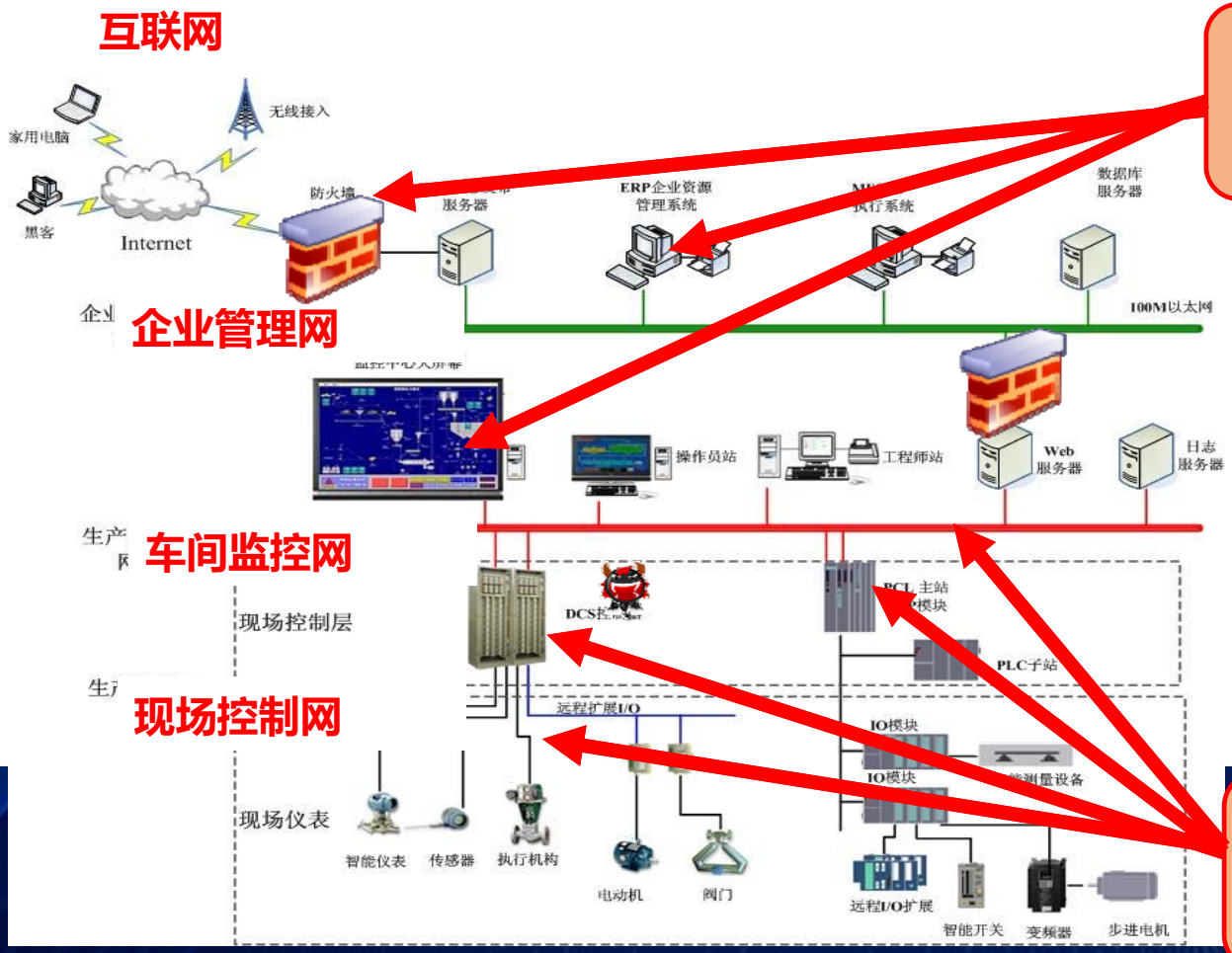


一、事件回顾

二、一些思考

三、一点建议

目标：“确保安全”



针对运载部分
准确认别，提前预警，实时防范

“外贼”
“内鬼”
都要防

针对内置、预埋代码
及时阻断，切断危害、确保安全

重点解决：“四高一难”“两不得”“五何”问题

高专业性、高隐蔽性、高欺骗性、高精准性、难以追踪

面对运行中的重要工控系统，“碰不得，摸不得”？

攻击代码长何样？何时进来？如何触发？何时触发？何时离开？

三段“安全”

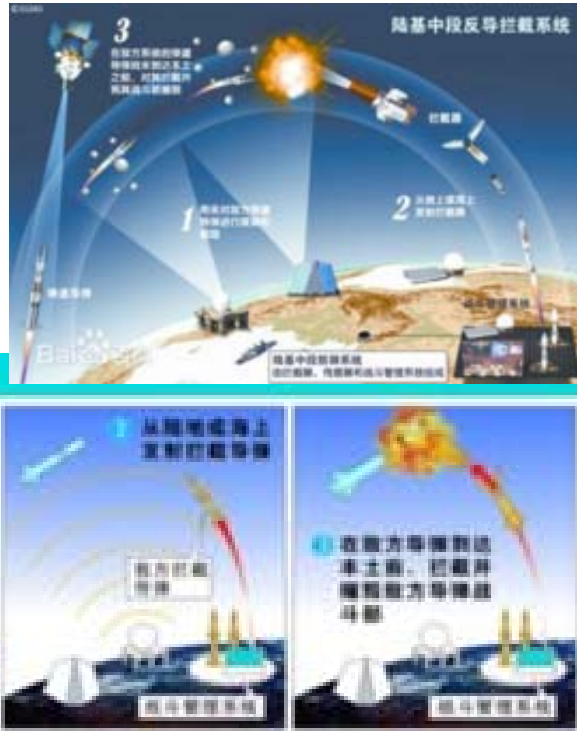
核心

工控安全

初始段：自主可控

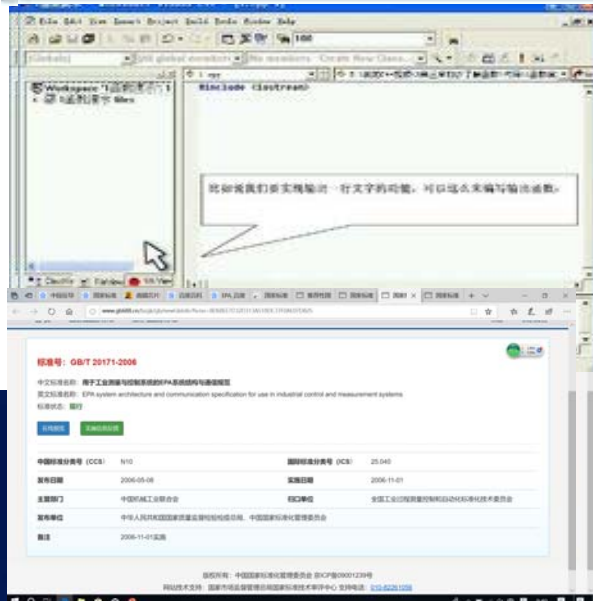
中段：运载拦截

末段：精准反制



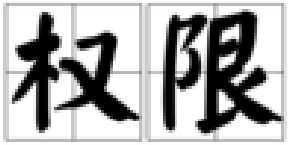
初始段：自主可控

- **硬件安全**
  - 自主可控安全芯片
- **软件安全**
  - 操作系统安全
  - 算法安全
  - 编程环境安全
  - 编译环境安全
- **协议安全**
  - 自主可控安全工控网络标准

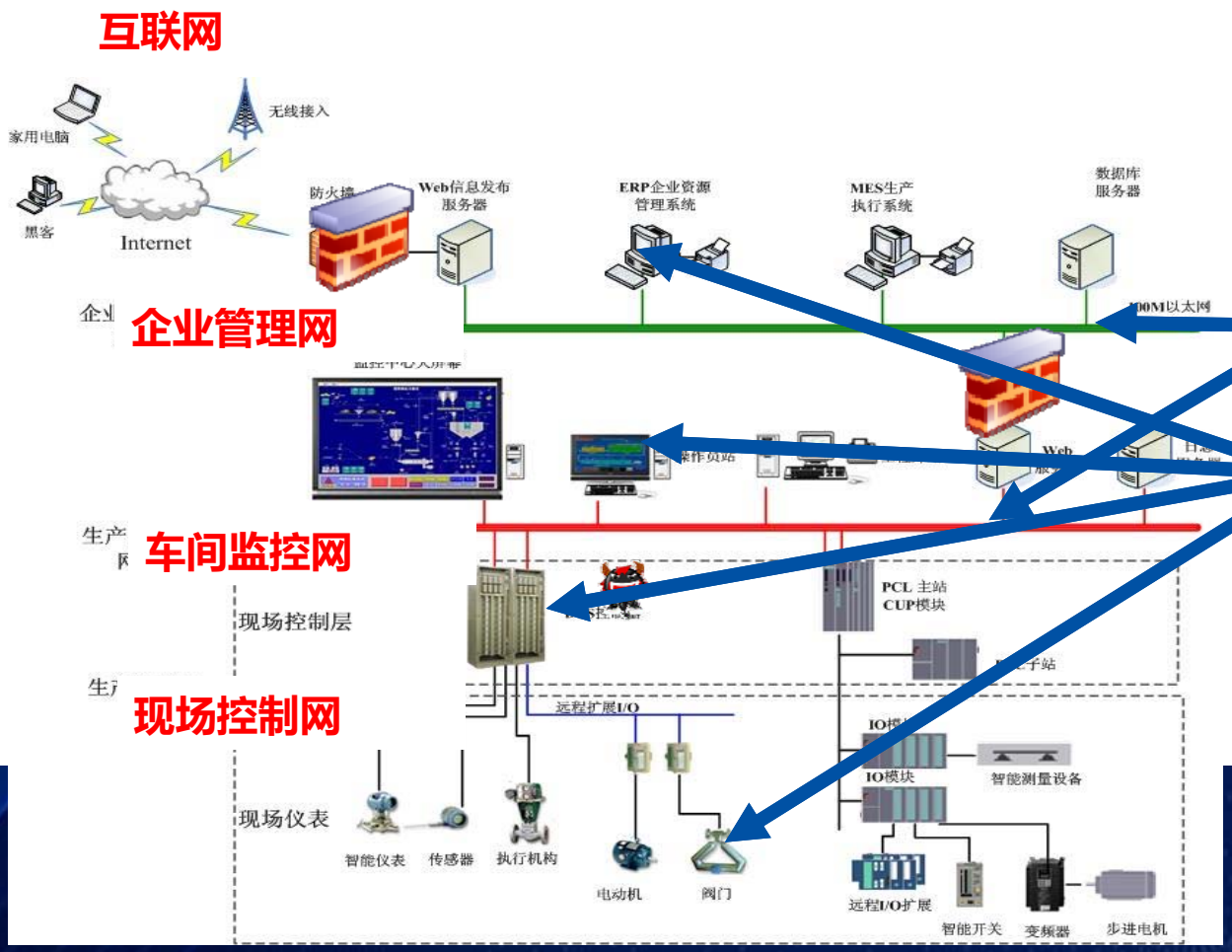


中段：
运载拦截

- 权限安全：获取、提升
- 软件安全：访问、修改、替换、调用等
- 接入安全：U盘、光盘、网络、无线等
- 应用安全：链接、邮件、木马、异常利用等



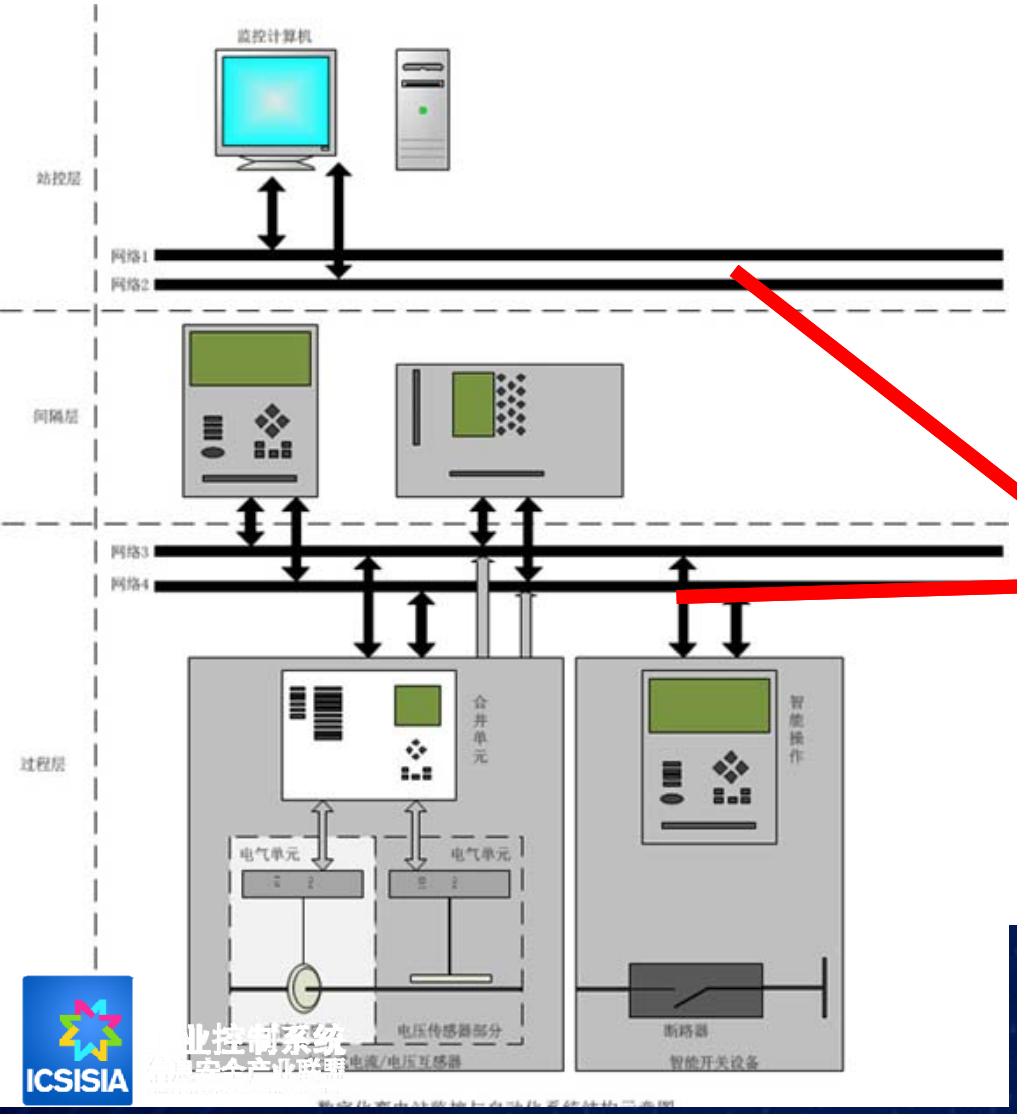
准确、正确识别“常规威胁” “核威胁”



末端安全：
生产安全
控制安全

1. 控制网络
2. 软硬件、嵌入式软件
3. 测量控制

“控制网络”安全



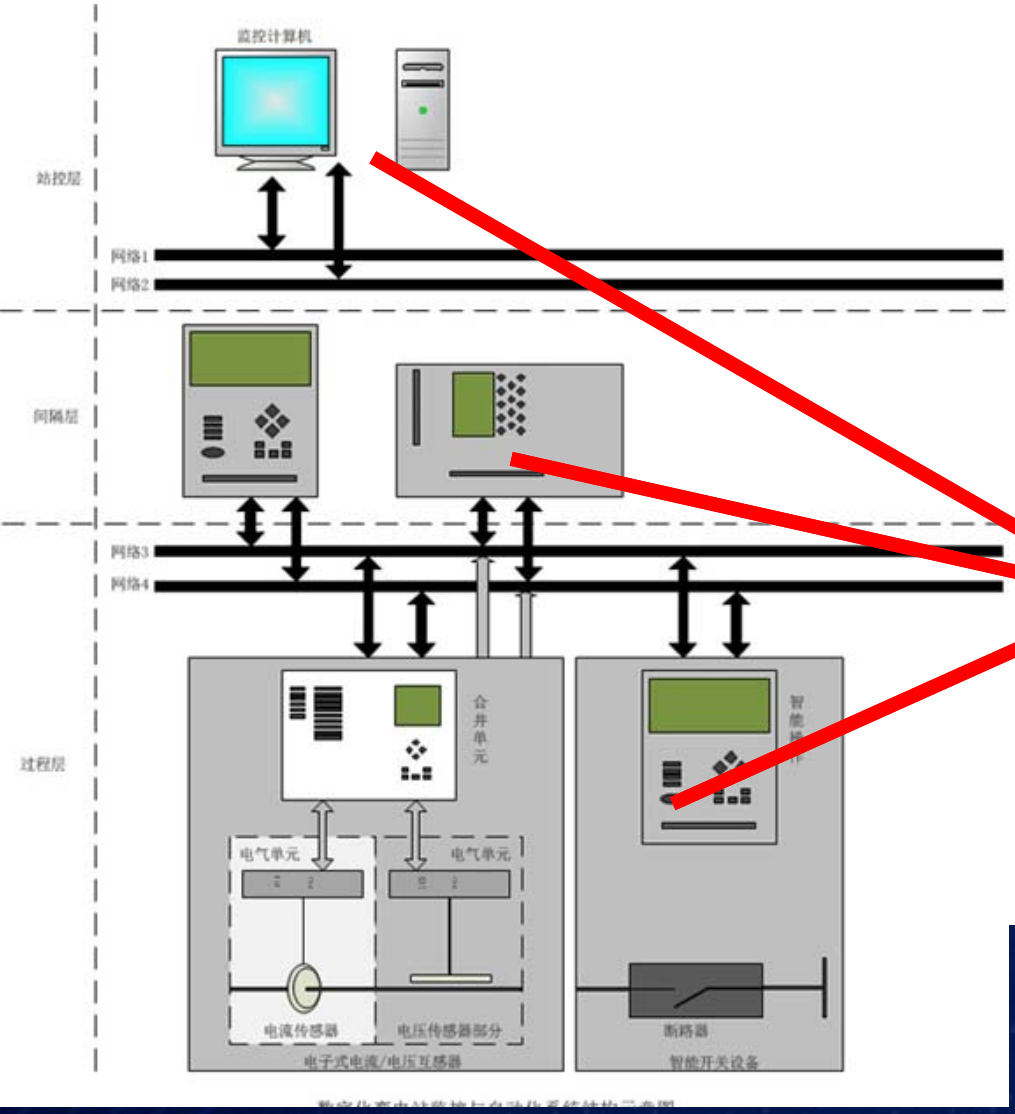
1

控制网络安全

- 行为安全
- 指令安全
- 操作安全
- 数据安全
- 状态安全
- 流量安全

ICSISIA

“软硬件与代码”安全

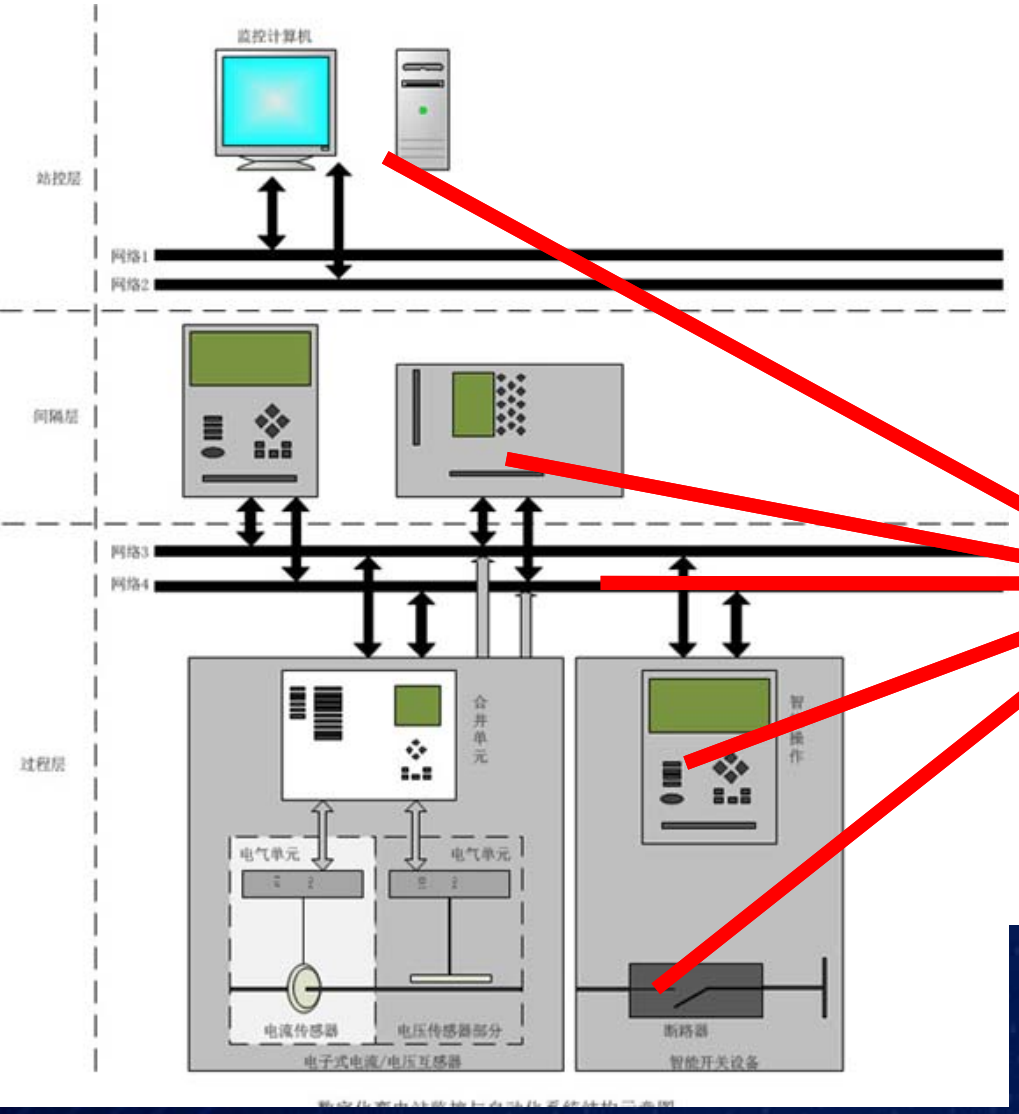


2

软硬件与代码安全

- 文件安全
- 函数安全
- 操作安全
- 调用安全
- 代码安全
- 更改安全

“测量与控制”安全

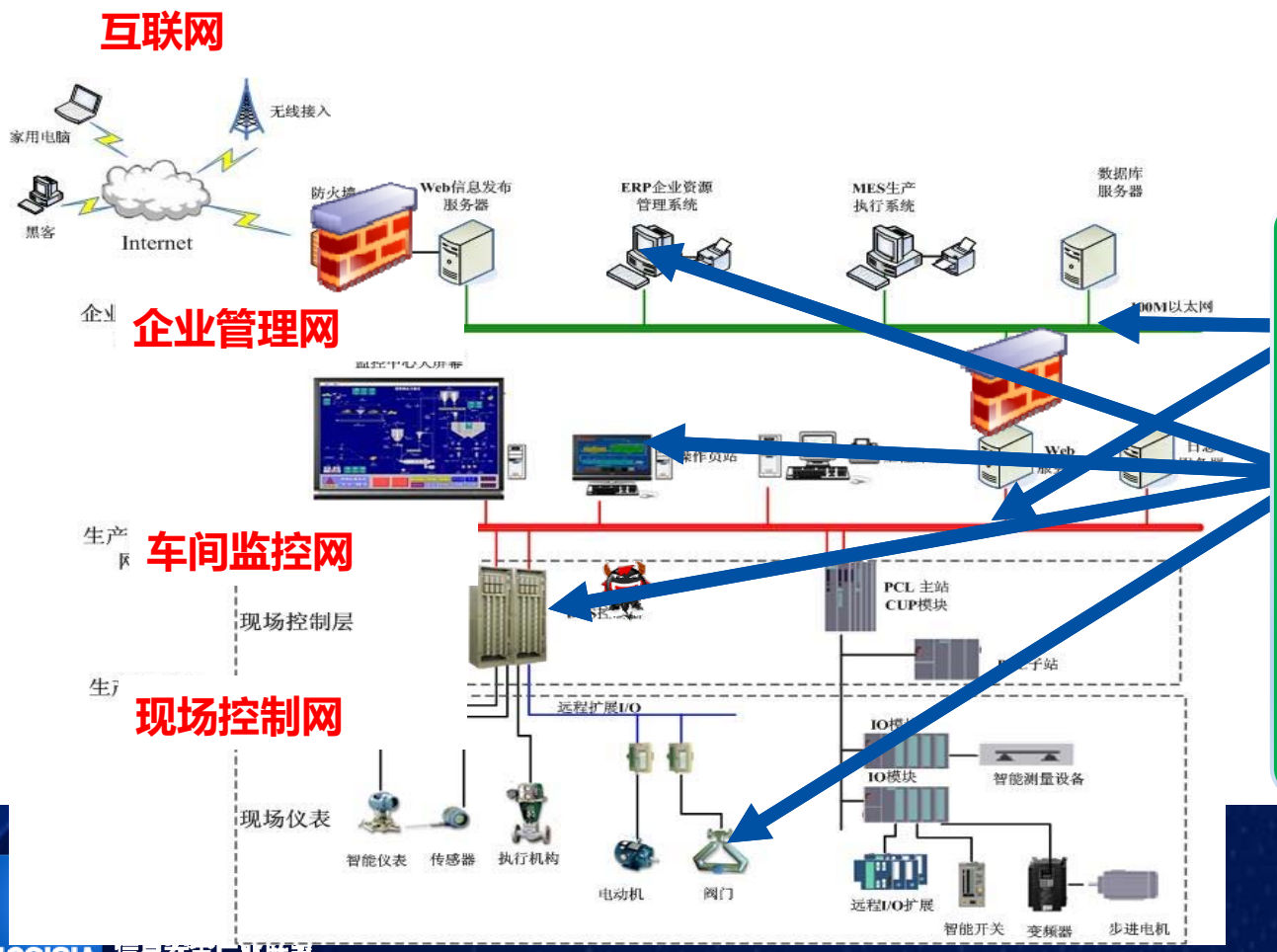


3

测量与控制安全

- **测量**安全
- **控制**安全
- **方案**安全
- **操作**安全
- **工艺**安全
- **流程**安全

应急响应与保障



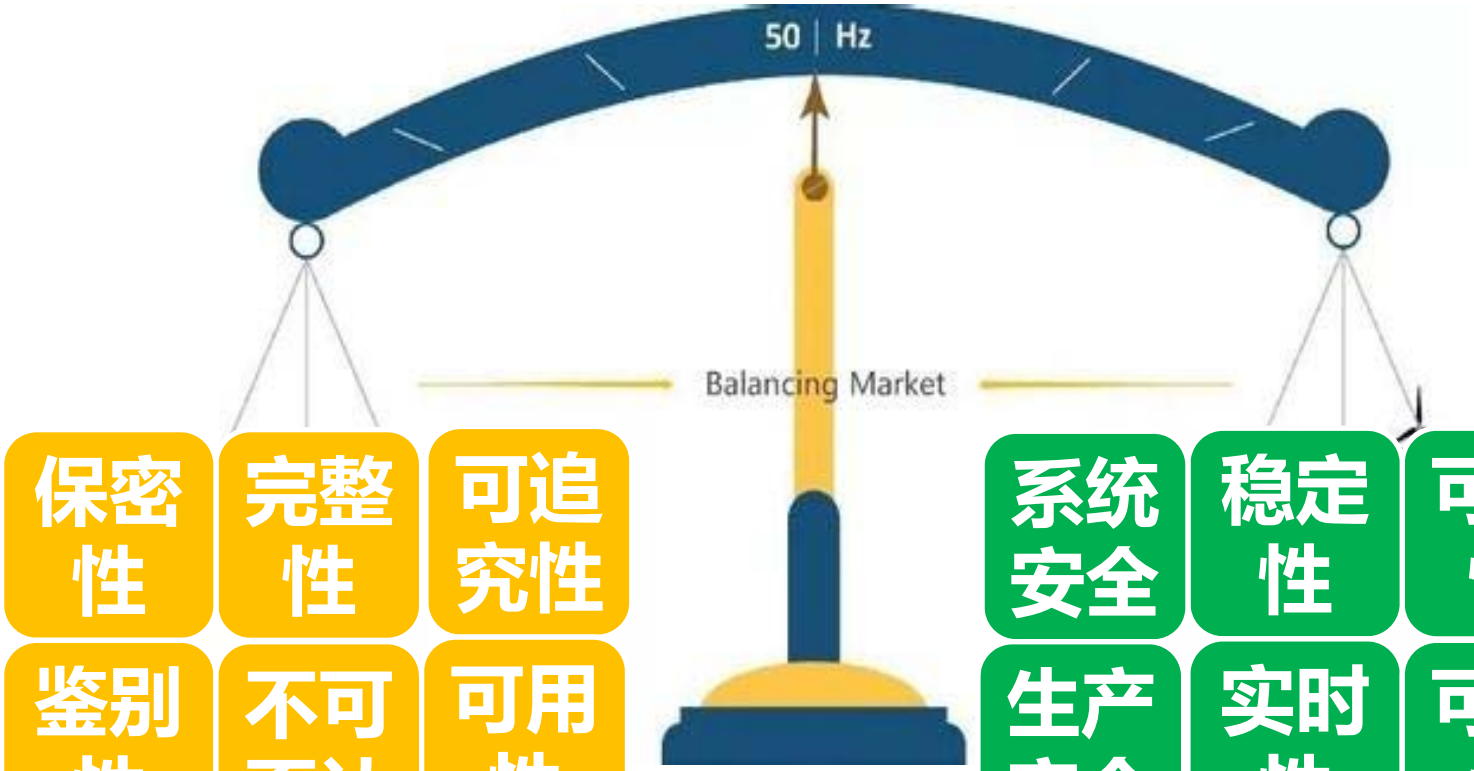
应急保障体系

- 紧急停车系统
- 紧急恢复系统
- 应急响应决策
- 应急响应指挥

检测、评估模型与理论

可观?	状态
可测?	行为
可看?	结果

网络安全与控制性能平衡?



保密性 | 完整性 | 可追究性
鉴别性 | 不可否认 | 可用性
可追踪性 | 可控性 | 可靠性

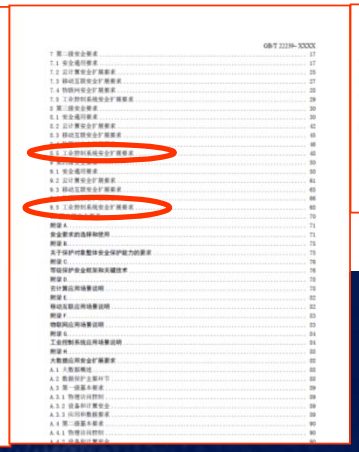
系统安全 | 稳定性 | 可用性
生产安全 | 实时性 | 可靠性
应急安全 | 鲁棒性 | 应急性

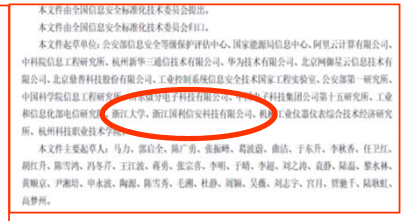
标准落地

主持制定工控安全国家标准5项

1. GBT/33009.1 工业自动化和控制系统网络安全集散控制系统（DCS） 第1部分：防护要求
2. GBT/33009.2 工业自动化和控制系统网络安全集散控制系统（DCS） 第2部分：管理要求
3. GBT/33009.3 工业自动化和控制系统网络安全集散控制系统（DCS） 第3部分：评估指南
4. GBT/33009.3 工业自动化和控制系统网络安全集散控制系统（DCS） 第4部分：风险与脆弱性检测要求

5. 《信息安全技术 网络安全等级保护要求2.0 第八章工业控制系统安全扩展要求》





控制系统
全产业联盟


ICSISIA
工业控制系统
信息安全产业联盟
Thanks