工业控制系统的信息安全问题日益凸显

罗安
北京和利时系统工程有限公司

对工业控制系统的基本功能要求

- 保证被控系统/设备连续、正常、安全运行。
- 不断提高产品质量。
- 保证生产操作人员的人身安全。
- 不断提高生产效率。
- 不断降低生产过程的能源、材料、自然资源的消耗。
- 不断降低生产过程的污染排放。

工业控制系统发展历程

- 基地式仪表——局地控制，检测与控制一体。
- 气动单元组合仪表——可组成系统，用气流传递信号。
- 电动单元组合仪表——可组成系统，用电流传递信号。
- DCS——数字化的控制系统，通过网络传递数字化后的信号。
- 继电器组合逻辑——用电气接点的通/断实现逻辑控制，通过电气连接线传递逻辑状态。
- PLC——用数字处理器实现逻辑控制，通过网络传递逻辑状态。
- SCADA系统——通过局域网或广域网将广泛分布的检测信号、逻辑状态集中到控制中心，实现集中监督控制。

信号传递技术的演进及其产生的问题

- 早期基地式仪表不存在信号传递问题。
- 在使用单元组合仪表构成系统阶段，使用物理或电气连接传递模拟信号。
- DCS、PLC、SCADA等现代控制系统使用网络（局域网或广域网）传递数字化后的信号。
- 数字化、网络化（即信息化）以后，产生了信息安全的问题：
  - 如何保证信息的正确性、及时性、保密性；
  - 如何防止信息被窃取、被篡改、被滥用；
  - 如何防止伪造信息的入侵、大量垃圾信息的攻击……。

信号处理技术的演进及其产生的问题

- 早期的控制系统采用物理技术进行信号的处理，如射流技术、模拟电路、开关电路等。
- 现代控制系统全部采用软件技术进行信号的处理，包括控制计算。控制领域已全面采用了信息技术。
- 完全依赖软件的控制系统面临的问题：
  - 分立元件的并行处理变成了数字处理器的并行处理，实时性下降；
  - 软件的执行在受到干扰或破坏后其行为及造成的后果难于预测与控制；
  - 软件的执行难于观察、控制和约束，软件Bug几乎无法根除。

信息安全与功能安全

- 信息安全——Security
- 信息安全的关注点：
  - 控制功能的实现；
  - 防止外界利用信息技术（如网络攻击、病毒、篡改或伪造数据等）破坏控制功能的实现；
  - 防止无意或有意的错误操作、超越权限的操作等造成系统控制功能的异常；
  - 防止保密/敏感信息泄露。

- 功能安全——Safety
- 功能安全的关注点：
  - 控制功能的实现；
  - 在受到外界干扰时、系统自身硬件出现故障时、受到自然灾害或人为的破坏时，必须保证最关键的功能不丧失。
  - 在极端情况下，控制功能完全丧失时保证被控系统处于安全状态。

小结：

- 功能安全（Safety）关注的问题：
  - 对信息处理系统的保护
- 信息安全（Security）关注的问题：
  - 对信息内容本身的保护
- 最终目的只有一个：
  - 保证系统功能的正确实现

实际应用和技术发展对控制系统的影响

- 通用信息技术越来越多地应用于控制系统，如图形用户界面GUI 、对象链接嵌入OPC、分布式组件对象模型DCOM等，这些技术的应用大大加强了控制系统的功能和性能。
- 控制系统的深入应用使用户对系统提出了越来越高的要求，更大、更快、更全、更可靠、更安全，已成为广大用户和厂家的不懈追求。
- 多系统互连已成趋势，消除“信息孤岛”已成为普遍要求。

信息孤岛与信息安全

- 控制与管理一体化进程的不断推进，信息技术的不断发展，使多年来困扰工控界的“信息孤岛”问题得到了很大程度的解决，但同时产生的信息安全问题也日益突出。
- “信息孤岛”的消除依赖网络的广泛应用，而网络正是信息安全的薄弱环节。
- 消除“信息孤岛”势必使工业控制系统增加大量的对外联系通道，这使得信息安全面临更加复杂的环境，安全保障的难度大大增加。

影响信息安全的因素

- 信息通信（有线与无线）。
- 人因（有意和无意的破坏）。
- 组态数据与下装。
- 通用的软件、网络协议、系统平台所引入的黑客攻击、病毒等。
- 管理漏洞及信息安全意识的淡薄。

工业控制系统与信息系统之异同

工业控制系统

- 局域网由专用网络逐步向工业以太网统一；
- 远程通信利用电信骨干网；
- TCP（UDP）/IP兼容；
- 网络拓扑基本固定，网络节点基本确定，网络传输的内容及传输时间基本确定；
- 每次传输的数据量有限，但次数频繁，实时性要求高；
- 软件系统确定，较少改变。

信息系统

- 局域网基本上全部采用以太网；
- 远程通信利用电信骨干网；
- TCP/IP是通用的基础协议；
- 网络拓扑不固定，网络节点不确定，网络传输的内容及传输时间不确定；
- 信息量大但对传输时间不作严格要求；
- 软件系统庞大复杂，经常改变。

控制系统的信息安全应有专门解决方案

基于控制系统与信息系统不同的特点，在解决信息安全的方案上应有所不同：

- 技术措施必须简单易行，力求不影响系统实时性；
- 在保证系统功能和性能的前提下，尽量减少通用信息技术的使用；
- 对控制系统与其他系统的信息传输进行适当限制，如单向通信等；
- 加强信息安全管理，采取技术措施与管理措施相结合的方法；
- 制定应急预案，在出现信息安全问题时及时补救。

安全管理

- 信息安全的特点是存在大量的人为因素，大多数信息安全问题是出于恶意的故意行为。
- 从理论上讲，控制系统的信息安全问题没有百分之百的保证，特别是对人为的恶意渗透或攻击。
- 在信息安全方面，技术措施只占三成，而安全管理要占七成。

安全文化

- 对信息安全的认识逐步提高，在相当长的时间里，多数工业控制系统的使用者不认为自己的系统存在信息安全问题，目前正在逐步缓慢地提高认识。
- 控制系统的生产厂家和集成商已开始重视信息安全问题，但成本的压力导致安全保障措施难于真正实施。
- 迫切需要国家层面采取强制性法规，对重要控制系统进行审核认证，提高信息安全保障水平。

Q & A

Thanks!