中国石油石化企业工控安全技术

（视频）交流会

2021年1月20日-21日

主办单位： 中国石油学会石油储运专业委员会
中国石油工程建设协会信息与自动化专业委员会




工控网络安全实施中应避免的误区

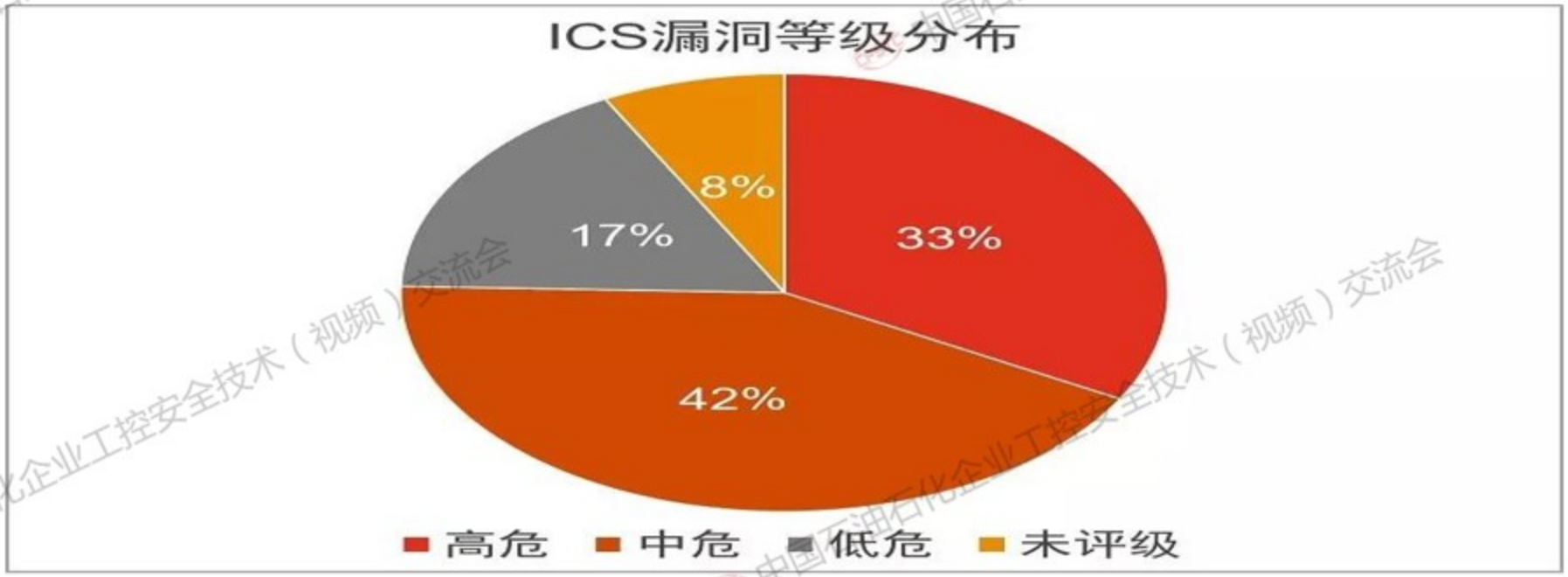
2010年，伊朗震网病毒事件爆光，揭开了工业控制系统的“神秘面纱”，也拉开了攻击工控系统的序幕。随后十年间爆发了众多与工控系统关联的安全事件。

2015年12月，使用专网的乌克兰电力监控系统遭到“Industroyer”恶意代码的攻击，导致7 个110KV 变电站和23 个35KV 变电站出现故障，80000 用户断电。

2017年12月，一种针对Triconex安全仪表系统控制器（SIS）的恶意软件TRITON被发现。恶意软件能修改安全仪表系统（SIS）的表决机制，从而使安全保护功能失效。

此外，由于工控系统在操作人员的界面软件使用了微软操作系统，因此针对互联网、计算机操作系统攻击的病毒（如勒索病毒WannaCry）对工控系统也产生了一些影响。事件表明，网络空间的安全威胁已从传统的互联网、计算机等虚拟空间迅速延伸扩展至物理世界的工业控制系统。即“计算机病毒”可以在不破坏工控系统本身的情况下，通过操控工业控制系统，引发装备损毁、生产中断、环境污染等，甚至可以引发灾难事故，导致社会动荡，安全生产受到了极大的威胁。工控系统已成为网络空间安全越来越重要的新战场。

依据CNVD公开披露的工控系统漏洞数据的统计分析，截至2019年4月已识别2,743个工控系统漏洞，其中高危漏洞907个(占比为33%)，中危漏洞1,163个(占比为42%)。



图二： ICS漏洞等级分布。 来源： CNVD官网

中国石油炼化系统使用的仪表控制系统的89%和电气继电保护装置的58%依靠进口。同时，随着智能化改造进程，工控网络从开放走向互联，网络安全威胁加剧，如： 2019年01月，某炼化企业催化装置停车并无法运行。原因是催化装置主风机和备用风机继电保护装置为国外产品， 2010年10月投运；全厂通讯管理机为国产产品，2018年10月投运。由于通讯管理机的MODBUS通讯对微机综保发送“对时”报文寄存器地址错误（正确对时报文地址应为0800H，但实际为012BH），“对时”系统对微机综保寄存器的关键数据进行随机修改，使继电器参数R1-R6出口随机“取反”，接点由常开转为常闭，继电器出口动作导致主风机跳闸，备机无法启动运行。

工控网络安全威胁主要来自以下几个方面：

（1）来自网络的远程攻击，如通过互联网、企业内部网、无线网，黑客和攻击者就可以远程对工控系统实施攻击；

（2）通过移动介质的带入攻击，如移动硬盘、U盘、光盘、移动终端等；

（3）预埋代码的潜伏式攻击，途径有工程实施时的预埋、通过维修维护带入的预埋等等。

从技术上看，工控系统所面临的网络安全威胁来自于两个方面：一个是传统的网络安全威胁，即利用操作系统、应用软件的漏洞发起的攻击威胁。这类威胁主要是针对计算机操作系统和应用软件的漏洞，获取计算机操作权限，或窃取隐私及敏感信息。

另一个更重要的安全威胁来源于对工控系统及其所控制的生产装置、生产工艺非常熟悉的有组织的攻击。从公开的资料可以发现，“震网”虽然利用了操作系统的漏洞，但这些漏洞只是被用于“震网”代码的传播，其核心代码却是利用了西门子控制系统和核设施的特性，而发起恶意操控，同时向操作人员发送欺骗信息。

我们对工控安全的理解，一是还停留在互联网安全和协议层面。 由于工控系统大多是由传感器、控制器、执行器等构成的闭环系统，其操控软件是供操作员进行工况监视和操作，工控协议是用于传输生产过程中的数据。因此，工控系统的网络安全需要从工艺技术等所有要素以及装置本身进行综合考虑。二是对工控安全恶意代码攻击原理和机制的了解有限。如今，各种社交媒体文件、文章、报告对工控安全事件的报道多、技术性分析少；对工控安全网络部分威胁的渲染多，对工控内部的威胁分析少；对操作系统“漏洞”介绍多，对工控系统自身软硬件以及工控网络漏洞分析少；

对操作系统、邮件等的漏洞介绍多，对工控恶意代码“长什么样，什么时候来，什么时候触发，如何触发”等技术问题研究少，导致工控网络安全工作的开展难以深入。三是工控安全的实施难以得到工控设备生产企业的配合。由于工控系统不同于互联网、信息系统，不仅要保证生产过程按设计要求运行在预定的工况，同时还要避免安全事故的发生。也就是说，工控系统的生产企业不仅要对生产过程的连续性、可靠性负责，还需要对生产的安全负责。这是传统信息安全生产厂商和安全产品难以做到的。

工控系统网络安全实施需要注意避免的几个误区

(1) 过于强调基于漏洞扫描的安全防护

工控系统设计开发关注的是如何使产品运行的可靠性和可用性高，对网络安全关注较少，因此其软件、硬件都存在着这样或那样的漏洞。然而，目前市场流通的漏洞扫描产品仅仅能发现引发工控系统溢出、宕机的漏洞，而像“震网”、Industroyer、TRITON那样所能利用的漏洞，还难以发现。

（2）过于强调补丁升级管理

众所周知，由于工控系统的软、硬件之间的结合紧密，使用了大量非私有的协议、技术和功能模块，一旦没有经过严格测试而给系统打补丁或者版本更新，轻则导致蓝屏、重则导致组态监控软件不再可用，极易导致生产中断。因此，对于一些重要、尤其是核心基础设施的工控系统，打补丁、软件版本更新必须慎之又慎！

（3）过于依赖工控系统的隔离安全

随着“两化融合”的不断推进，生产系统与管理系统的互联已经成为工控系统的基本架构，与外界完全隔离已不可能。另外，GPS时钟对时、无线仪表和维护用的移动设备或移动电脑等，都成为了代码带入的工具。

（4）过于高估工业防火墙等传统防护产品的作用

从目前工控系统的实际来看，工控系统除了它支持的协议之外，其他所有的协议都会被过滤。也就是说，工控系统一般都具备了一般防火墙的能力。从这个意义上看，目前市场上所谓的工业防火墙，也仅仅起到应付检查的自我安慰作用。

(5) 过于依赖单向通信隔离装置

针对工控系统的攻击途径有多种，有通过网络远程实施的，有通过无线接入的，还有通过移动介质、工程实施与维保预埋等途径，单向通信隔离装置也只能起到部分作用。

从具体实践来讲，对工控系统的网络安全防护和保护需要综合考虑：

一是需要覆盖工控系统软、硬件等所有部件。

二是需要结合技术工艺特点与生产操作流程而开展。

三是需要覆盖工控系统的设计、生产、调试、工程实施、运行维护、维修等全生命周期的所有环节。

工控系统的网络安全防护和保护是一个极其复杂的系统工程，需要回归控制系统的初心、回归控制系统的本质，从工控系统的软、硬件、网络以及技术工艺、设备、生产流程、生产装置等多方面同时着手，才能真正有效的实现工控网络安全防护和保护。

不妥之处，请批评指正！谢谢！