自主可控——工业互联网的安全阀

编者按：工业互联网作为新一代信息技术与制造业深度融合的产物，近年来呈现出蓬勃发展之势，但随着越来越多的工业控制系统及设备与互联网连接，开放互联的环境使工业互联网安全问题日益凸显。据统计，在过去一年，国家信息安全漏洞共享平台收录了 100 余个对我国影响广泛的工业控制系统的软件安全漏洞。工控安全的发展与研究是工业互联网安全的关注重点之一。在中国信息协会信息安全专业委员会 2018 年会暨第八期网络安全创新发展高端论坛上中国电子信息产业集团有限公司第六研究所副所长、工业控制系统信息安全技术国家工程实验室常务副主任张尼强调了自主可控对工业互联网安全的重要性，本刊撷取部分内容，以飨读者。

工控系统的趋势与挑战

工控系统分为离散控制、过程控制、运动控制三类，工控系统广泛应用于能源产生与输送分配，例如：交通行业、物流行业等大量使用的都是这种控制系统。在前工业 4.0 时代对于安全的考虑非常少，这主要源于两个前提假设，一是物理隔离，二是所有协议、业务逻辑相对简单。工业 4.0 时代，随着智能化、信息化的发展，更多的软件联网、终端与云连接，当各种终端与网络连接，安全问题则需要高度重视，如何安全保护我们关键的基础设施？

首先，从顶层开始，国家越来越重视网络安全问题。无论是法规、指南、计划等都将公共安全提升到国家战略层面。科技部连续两年将工控系统安全当作网络空间安全的重要方向。

当前工控系统的安全面临诸多威胁与挑战。第一，最主要的挑战是工控系统成为国家级黑客的主要目标。攻击工业控制系统不是病毒，而是网络武器。第二，核心技术的自主掌控。第三，工业终端从闭环走向开环，这是一个新问题。随着新技术不断演进、更新换代，必然面临着安全的阵痛。第四，工业互联网的安全仿真环境。工业环境门槛高，测试平台的搭建成本高。第五、工业大数据。大数据平台是互联网化的，有存储、采集、挖掘、分析、发布、共享一系列的流程。对工控系统来说，这种开放互联的环境对工业互联网的安全来说都是挑战。

云计算、大数据、物联网增加了工业处理流程的开放与不确定性，安全风险进一步集中，工控系统的安全不是一个小安全的概念，而是需要一个深度的安全防御体系。

安全防御策略

面对诸多挑战，如何应对？

第一，自主可控，不是网络安全的概念，是一个大安全的概念，是安全的外延。谈自主可控，大家都非常支持，但是落实到自身实际很难实现。自主可控并非所有都自主可控，全球的工业发展是一整个的产业，是允许产业之间交融的，所以核心的东西我们需要自主可控。

第二，自主可控的关键还表现在维护升级不受制于人，卡脖子、牵鼻子的状态必须要摆脱。例如：设备层面一些小的设备、智能化的设备、在现场起关键作用的设备尽量用自主可控的东西替代。PLC、交换机、路由器、服务器都是关键的、核心的网络设备，这些都需要自主可控。

第三，自主可控不等于安全，事前的态势感知是安全防护的一环。工业安全设备有很多专业经验和知识，安全防护一定要结合每个行业的业务。

一方面是信息的安全，一方面是自主可控的安全，两条路融合之后要经过若干年，达到一种平衡，我们可以一边发展、一边能够保证安全，现在的安全保障不是保障不出故障，而是保障不被敌对势力盯上。

总体而言，自主可控的关键是应用。大规模的应用，一定要有真正的用户，安全设备，用得越多才证明越可行，才是真正落地。信息安全一定要与现场安全痛点相匹配，安全要同步规划、同步建设。