



工业网络安全纵深防护建设

文/剑思庭 罗克韦尔自动化（中国）有限公司

文章分享的内容主要包括工业网络中攻击基础设施的技术路线，以及工业自动化控制系统如何基于这种攻击技术路线构建纵深防护体系。

工业网络攻击基础设施的技术路线

攻击一个基础设施分以下几步：

第一步是锁定目标，找到要攻击的厂商，一般都是制造业的工厂。找到厂商之后，通过厂商发布的信息来锁定其所使用的是哪个厂商的控制系统，通过建设年限和厂商就能够锁定当时构建设

备的版本。同时可以登录一些专门公布漏洞的网站，通过检索厂商的名字和版本，可以搜索到它是否有相应的漏洞。

第二步是在确定有漏洞的情况下联系制造商，最普遍、成本最低的方式就是通过招聘的邮箱，通过钓鱼邮件发送针对某一个控制系统采集或者是攻击的恶意代码实施攻击。

第三步，招聘邮件发给电气主管后，其中的木马程序通过电气主管的计算机攻击OT网络，进行信息的盗取，对控制系统进行恶意攻击，最后造成OT系统的瘫痪。传统的OT系统很少有网络链

接，随着IT和OT的逐渐融合，IT系统的风险也传导到OT系统。

2016年工业和信息化部印发了《工业控制系统信息安全防护指南》，关于工业控制系统信息安全在技术层面上有七条：第一是工业软件自身的安全和管理；第二是要做安全的配置，并且做好补丁的管理，补丁管理包含了操作系统和应用软件；第三是安全的防护边界，即自动化控制系统和办公系统进行对接的边界；第四是物理安全和环境安全，这个最容易被忽视，但如果做得好可以抵御很多层面的攻击；第五就是身份认证的相关程序要尽量完善；第六是OT系统与

IT系统对接后远程安全的访问如何构建；第七是对于深度包协议的检测，深度包协议检测主要指工业协议，传统防火墙基本上是4层，当然现在有很多7层的防火墙，但7层的防火墙可能更多地偏重于IT协议，对于工业协议的深度包检测还需要技术支持。

工业自动化控制系统如何构建纵深防护体系

公共系统里面的安全应该涵盖以下方面：第一是控制器；第二是数据中心，即技术架构；第三是网络；第四是终端；第五是移动端。自动化企业的标准架构为：最基础的是控制器，包括电器控制器和逻辑控制器，它们之间形成一个工业控制的环网，其中有分布式的交换机及工厂核心的交换机，也有一些人机接口，通过防火墙再去企业端。在这样非常标准的架构下如何设计最基本的防护体系？这其中有三类人要来共同起到防护作用。第一类人就是工业控制工程师。首先要保证控制器的安全，包含控制器的安全设置、物理保护、电子签名及加密通信；其次他们还要负责PC的安全，即PC本身的操作系统和应用软件的安全，以及一些应用的加密和加固；还有就是常规的工业交换机里面最基本的一些端口的安全，以及端口引入之后的一些认证和设置；最后就是工业防火墙的管理和设置。第二类人是工业IT工程师。负责工厂里面所有的自动化网络和安全建设，包括密码、注册表、核心路径、工业WiFi及访问的防护等级，以及持续危险检测并分析报警。另外，如果有企业外部的远程访问，要规定谁能做远程访问，以及能够访问哪些内容。第



剑思庭

罗克韦尔自动化（中国）有限公司
工控安全团队负责人

三类人是传统IT工程师。首先负责目录的部署，因为企业有自己的目录服务器，在工业系统里面要求目录统一安全管理，两级目录可能有联动。其次负责安全认证，安全认证系统和企业的认证系统一定是联动的，如果没有身份的安全认证，很难做到柔性化的管理。

另外，工艺安全隔离区除了防火墙之外，还有几个重要的事情要做。第一是所有操作系统的补丁，在这里面要有补丁服务器；第二是所有终端的防护，因为终端肯定是要通过企业的防火墙去往互联网及时更新；第三是要分析企业的业务，确定哪些业务与OT系统和IT系统进行连接。在这里面一定要做应用的镜像，做镜像最大的好处就是能够把端口和应用隐秘掉，还可以通过应用的镜像增加一层防护。否则的话，在防火墙里面只能完全对OT开放。

经过这样的纵深防护之后，系统就具备了基本的工艺安全的深度防御能力，对于攻击者，就已经有了比较大的阻碍。但也并不是说

这个系统就是铁桶一块，因为安全的建设与攻防永远是动态的，每天都在变化。那么，工业控制器和软件上面到底要做哪些安全防护？第一就是PLC的自身安全。一般PLC都有自己的固件，可以选择一个版本，同时还可以选择加入电子签名，防止其他人通过其他的路径来访问控制系统。可以定义所有的可访问的标签，哪些是可读的，哪些是可写的，减少攻击面，信息被读取就是信息泄露，如果被控制就可能造成人机危害。

另外，上位机需要在应用软件上面做详细的设置。如哪些报警和通信谁能访问？哪些控制组谁能创建？哪些标签谁可以访问？对这些做详细的规划之后，就可以做成一个最小访问路径。否则的话就只能分成两种：一种是维护人员；一种是操作人员。维护人员是全部的权限，操作人员也具备全部的权限，那么这两种权限就分不清了。一旦攻击者获得了一个操作员的权限，就可以为所欲为，所以，一定要把基本的工作做好。

在基础网络的设施里面出现最多的是交换机，而不是路由器。防火墙基本上不是在最末端，就是在边界端，中间层都是以交换机为主。交换机是被自动化人员长期忽略的一个设备。自动化人员一直把交换机当一个HUB来使用，网线一插就结束了，就看能不能通。但是，对于交换机攻击的方式方法太多了。比如最原始的泛洪攻击，当向交换机成批量发送毫无意义的地址表时，交换机查不到地址就会做泛洪发送，这时攻击者可以轻松看到相关信息。

针对安全基础设施存在的问题要采取哪些保护措施？首先是应该把所有不用的端口封掉，端口



起Power Security作用，可以锁IP和MAC地址，锁MAC地址在工业系统里面是经常用的一种方式，这样的话泛洪攻击等就会失效。

安全身份的认证系统是很关键的，比如一个外面的供应商要访问系统，不能直接访问下面的设备，而是先要进入认证系统，获得系统认证之后才能访问某一个控制器，这个认证是必须具备的。否则，由于传统的自动化系统是设备直接插到交换机上，外部供应商可以看到交换机上的所有设备，如果这些设备没有加密，外部供应商就可以把程序、配方甚至是用户的业务数据全部拿走，造成比较大的危害。如果攻击者是一个黑客，随便找一个在边缘端的交换机插上去，就可以在这里面为所欲为，这是一个非常大的危害，所以一定要有身份认证系统，身份认证不合格的时候就不能访问，同时这个被攻击的端口还会被记录。

另外，远程访问时如何从互联网端跳转到最下面的控制系统？首先要有一个安全的远程访问的Server，放在工业安全隔离区里面，通过一个企业的VPN拉

进来，里面有自己的Auditor、认证和审计系统，然后去设置哪些资源是可视的。再继续往下跳到Size模式下面，才可以访问控制器，也就是说它要经过两级的防火墙才能进入到最底层。同时，这里面还要有认证和资产方面的管理，Auditor要能够支持工业协议。

工业安全隔离区最主要的作用是把下层的应用安全地释放给上一层，同时也让上一层的一些信号有效地进入到下一层。把一些外部的数据经过外部代理再释放上去，可以屏蔽最下层Web Server本身的架构，同时还可以随意指定一些外部的接口，在外部代理上面做一些外部上的防护。通过这种形式来加强IT和OT融合之后的安全。

物理安全和环境安全非常重要。现在大量的这种设备，如交换机不用就用堵头堵上，所有的网线都是插进去不能再拔出来，取出端口需要一些特殊的工具，这些很好地保证了端口安全和物理安全。还有就是通过一些钥匙锁把机柜门锁好。这种安全方式投资很小，特别适用于没有

安全人员的小型企业。

另外，工业防火墙对安全很重要，可以在防火墙里面制定策略，只允许进行数据通信，不允许对PLC进行上传、下载、开关和启停等，要支持深度包检查，能够分析出上位机对控制器所发出的指令，最后隔离恶意的竞争，保证整个控制系统的可靠性。

公共客户端的主机安全必须高度重视，因为工业控制系统50%以上的安全风险和安全事件都是由主机端产生的，主机端的安全防护是重中之重。之前比较旧的系统，其工业控制软件基本上都不对杀毒软件做任何兼容性的测试，因此它们没有办法安装杀毒软件，只能采用主机白名单这种防护方式。随着杀毒软件逐渐和工业自动化厂商进行联动，一些大厂商的自动化软件已经做了很多的杀毒软件的测试，可以把AV直接引进到防护端里面。还有一种也是现在最流行的EDR防护方式，直接对终端做防护，可以联动云端，可以做一些零类的捕捉。除了这些之外，还可以对USB做一些防护，防止USB设备遭受攻击。最后，把工业控制系统里面所有设备的流量映射到工业威胁检测系统里面，通过相关的事件分析有哪些威胁，再通过工业威胁检查系统自己的算法并产生报警，从而实现工业自动化系统的可视化管理。EA

（本文源自《2022数字化车间和智能工厂》在线论坛第三期：布局工业通信和5G+工业互联网，编辑整理：任智惠）



扫描二维码了解更多