安全人才能力发展中心

基于工业互联网控制设备“攻击方式”的研究

作者： 360 安全人才能力发展中心

摘　要：随着工业互联网的快速发展，工业互联网控制设备都具备了以太网模块。传统的信息孤岛，已经成为了一网到底的全面网络设备。我们通过对控制设备网络攻击方式的研究，对其武器化形式的探索，以控制设备现有的方式，将控制设备武器化。通过对控制设备武器化后，实现在内网中对其他设备进行网络攻击的研究。

关键词：工业互联网安全；控制系统；攻击方式；网络安全

目录

一、 工业互联网网络安全现状 1
1.1 工业互联网控制系统概述 1
1.2 工业互联网安全现状 1
1.3 典型工业互联网安全事件 1
二、 设备武器化研究必要性 2
2.1 防护角度 2
2.2 攻击角度 2
2.3 安全思维 2
三、 控制设备网络资源 3
3.1 编程语言 3
3.2 以太网模块 3
3.3 通信协议 3
四、 控制设备信息传播方式 4
4.1 控制设备作为核心，向外扩散进行数据传播 4
4.2 控制设备作为桥梁，进行数据传播 4
五、 控制设备信息传播实现方式 5
5.1 直接传播方式 5
5.2 代理人传播方式 7
六、 安全防护意见 10
6.1 网络区域访问控制 10
6.2 网络安全审计 10
6.3 协议深度解析防护 11
七、 研究环境介绍 11
八、 结语 11

一、 工业互联网网络安全现状

1.1 工业互联网控制系统概述

随着工业互联网的发展，促使工业企业在加快了数字化转型升级。数字化、网络化、智能化的生产方式成为了主流。大量的工业控制系统和生产设备通过互联互通的方式，连接了起来。这也使得这些重要的生产系统成为了黑客攻击的主要目标，并针对工业互联网控制系统发起了网络攻击事件。工业互联网控制系统的信息安全重要性日益凸显，成为了制造强国和网络强国建设的重要支撑、保障国家网络安全的重要基础。

1.2 工业互联网安全现状

工业互联网控制设备的安全偏向于功能安全、设备硬件安全、生产工艺安全等，但却很少关注控制系统本身的信息安全。如系统的固件、软件、网络等信息传递的媒介及途径。工业互联网控制设备一般都采用的稳定设备，运行时间长，生命周期比较长，因此这些设备的漏洞就成为了黑客被攻击的入口，也是信息安全的重要保护点。

但随着科技技术水平的发展，工业互联网控制设备的智能化、网络化和通用性的提升，控制设备的性能也越来越好，可完成的功能越来越多，导致信息安全防护的手段需要不断的提升。

本文主要从工业互联网控制设备角度出发，以控制设备中心，以不同的网络数据传输方式为契机，分析信息途径或者介质探索控制设备的信息安全。

1.3 典型工业互联网安全事件

“震网”事件，主要利用微软 Windows 系统和西门子 SIMATIC WinCC 系统的多个漏洞，通过移动存储介质和局域网进行传播，通过西门子控制器控制的变频器的信息被篡改，导致执行设备的损坏。

Havex 病毒事件，主要利用 OPC 协议的开放性，从控制系统中的 OPC 服务器，获取工业互联网生产现场的数据，进而影响生产现场。

Black Energy 恶意软件事件，主要利用了僵尸网络，以恶意代码攻击载荷的方式，远程控制工业互联网控制系统，直接控制工业现场的生产，导致大面积的停电事故。

以上这些工业互联网事件，都是从外部网络，入侵到工业互联网控制系统中，对控制系统中的控制设备进入攻击，进而造成影响实际生产生活的恶性网络攻击事件。

本文主要研究以工业控制设备本身角度出发，以网络、协议、控制等手段，实现将控制设备武器化，在内网中直接发起网络攻击，造成生产设施、生产工艺的停顿或者破坏。

二、 设备武器化研究必要性

设备武器化研究是通过研究设备不同的信息安全角度，以内部执行方式，将正常运行的设备，代替成网络攻击发起端，形成网络安全起点。

2.1 防护角度

在工业互联网高速发展的今天，防护手段也在不断变化。针对不同情境下的攻击手段，防护者所能思考，以及所能见到的攻击事件不断发生以及变化。主要分为以下几种情况：

1) 对已知的攻击手法、手段以及攻击方式的防护；

2) 对未知的攻击手法、思路以及安全隐患的安全加固；

3) 安全体系防护，如何寻找自身系统的靶标点、脆弱点等。

2.2 攻击角度

在“未知攻、焉知防”的理念下，通过研究各种攻击手段、手法以及路径的过程中，才能发现如何更好的防护系统安全。并可以通过提升研究方法、思路获得新的防护方式。

1) 分析攻击路径，探索安全防护壁垒；

2) 分析攻击手段，探索安全防护规则；

3) 分析攻击靶标，探索安全防护配置。

2.3 安全思维

安全思维是有效指导如何加强系统安全，在不断的更新攻击靶标、攻击手段和攻击路径，有效检验安全体系的合理性。通过不断的渗透测试、定向攻击和武器化进攻，不断冲击旧式

安全体系，不断提出合理的安全建议，优化安全策略，进而完善安全体系的建设。

三、 控制设备网络资源

控制设备的网络资源这里分为编程语言、以太网模块以及通信协议。以太网模块和通信协议是控制设备主要对外的服务资源。编程语言则是通过决定客户运行程序的主要资源。

3.1 编程语言

工业控制系统控制设备所运行的客户代码，一般都是由编程语言组成。根据国际电工委员会制定的工业控制系统语言标准（IEC1131-3）。控制设备的编程语言包括以下五种：梯形图语言（LD）、指令表语言（IL）、功能模块图语言（FBD）、顺序功能流程图语言（SFC）及结构化文本语言（ST）。

目前大部分的控制设备都支持以太网形式的网络使用，如西门子 PLC 的网络控制模块有 TCON、TSEND、TRCV 等，分别可以进行 TCP/IP 网络连接，发送网络数据包，接受网络数据等。可以充分利用这些资源使用控制设备对内部网络发起网络请求，已达到网络传播、网络攻击、网络数据分发等功能。

3.2 以太网模块

我们知道，大部分的恶意代码都需要网络进行传播或者触发。尤其僵尸网络，更是通过以太网将分散在不同区域的设备，统一执行命令操作。

随着工业互联网控制系统的联网化需求，大部分设备都已经自身携带以太网模块，或者根据需要可以配置以太网独立模块以进行联网的需求。

3.3 通信协议

控制设备的通信协议，是工控设备与工控应用、工控设备与工控设备之间沟通的一种重要语言。通信协议是双方完成通信或者服务所必须遵守的规则和约定。通过通信协议可以将更多的设备、应用互联起来。

控制设备的通信协议一般包括三个部分：协议格式、协议内容及通信方式；

协议格式，即我们经常讲的通信协议文本，它包含了协议格式和协议规范；

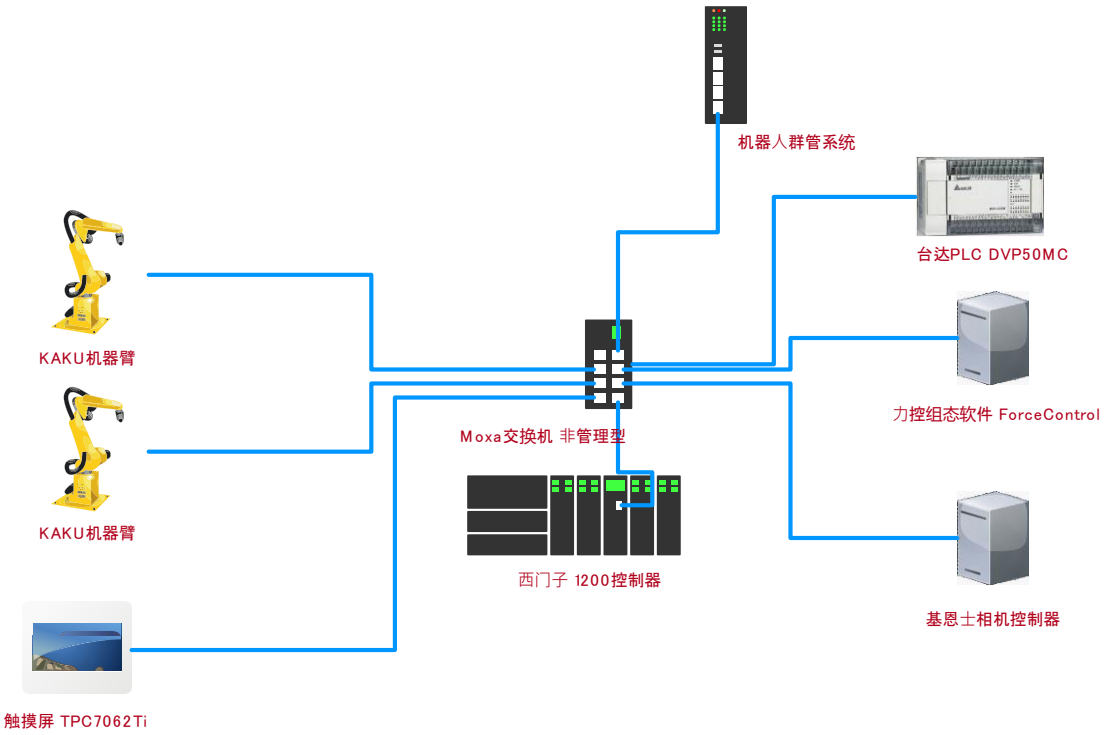
协议内容，在工业控制设备中，通常包含两个部分。一个部分是控制部分，另外一部分是数据通信部分；控制部分主要包括设备的配置信息，如 IP 地址设置、工程上传下载、设备状态的设定等内容。数据通信部分主要包括数据传输，包括读写数据、数据的交互及数据的处理等。

四、 控制设备信息传播方式

控制设备信息传播方式，这里归纳为两种：一种是以控制器核心的信息传播方式；另外一种是控制器为桥梁，进行信息的传递。

4.1 控制设备作为核心，向外扩散进行数据传播

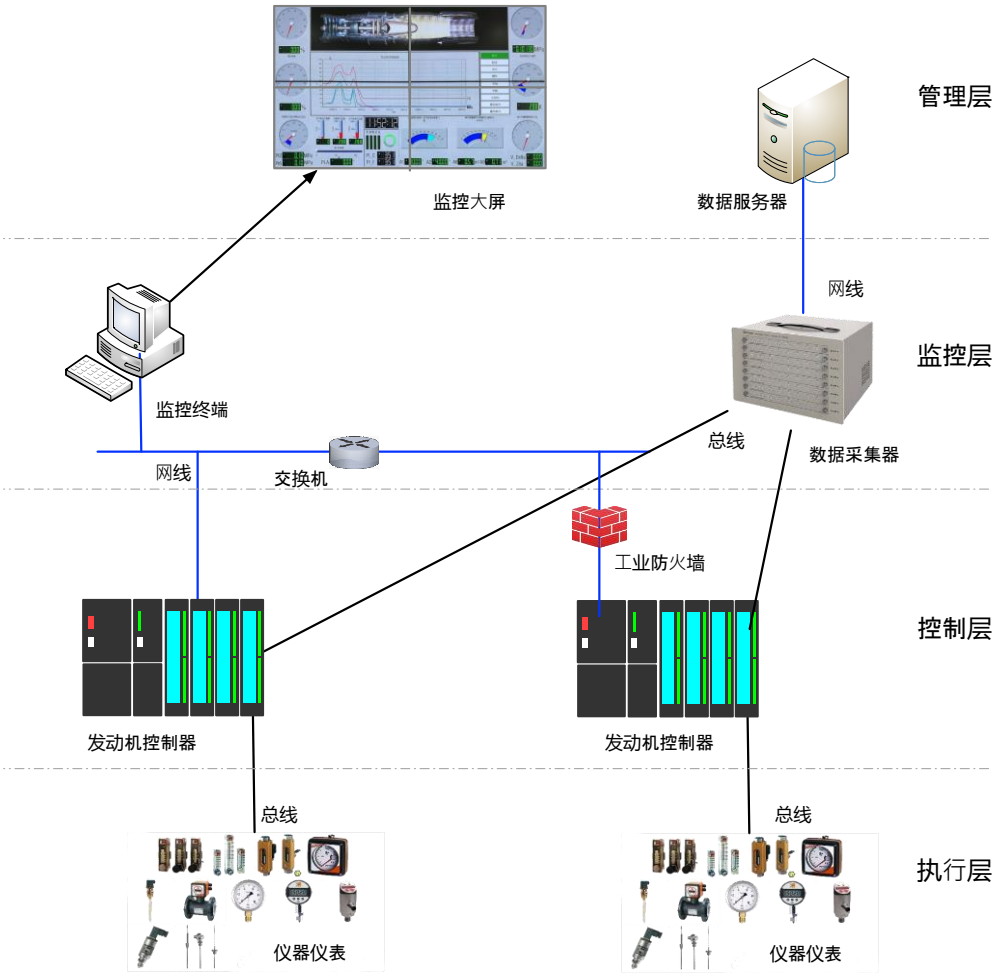
传统的智能制造行业网络结构拖，如下图所示：



上述网络中，是以西门子控制作为控制核心，执行逻辑控制。其工艺流程为组态软件或者云平台下发订单信息，控制器接收到订单任务，按照规定流程依次控制机械臂，相机，辅控 PLC 执行动作。并将执行的结果反馈到触摸屏、云平台及组态软件中。

4.2 控制设备作为桥梁，进行数据传播

桥梁式数据传播，其现实网络结构图如下图所示：



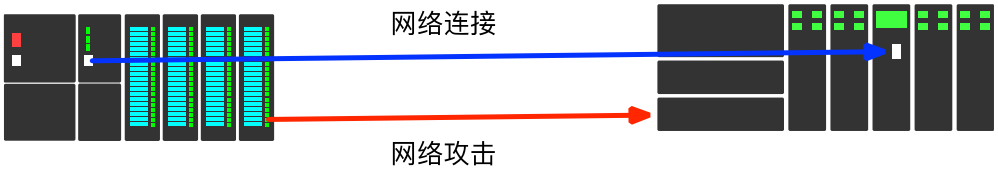
上述网络中，是以西门子控制作为桥梁，将底层数据，经过处理后，传递给数据监控大屏及数据服务器。其工艺流程是监控与监督现场执行层的数据，并将数据存储与展示。

五、 控制设备信息传播实现方式

控制设备信息传播实现方式采用直接传播方式以及代理人传播方式。

5.1 直接传播方式

直接传播方式采用 PLC 与 PLC 直接传播的形式，网络连接与数据传播如下图所示：



网络连接：网络连接通即可。

网络攻击方向：是 PLC 与 PLC 直接发起攻击。

直接传播方式的实现逻辑如下图 1 所示：

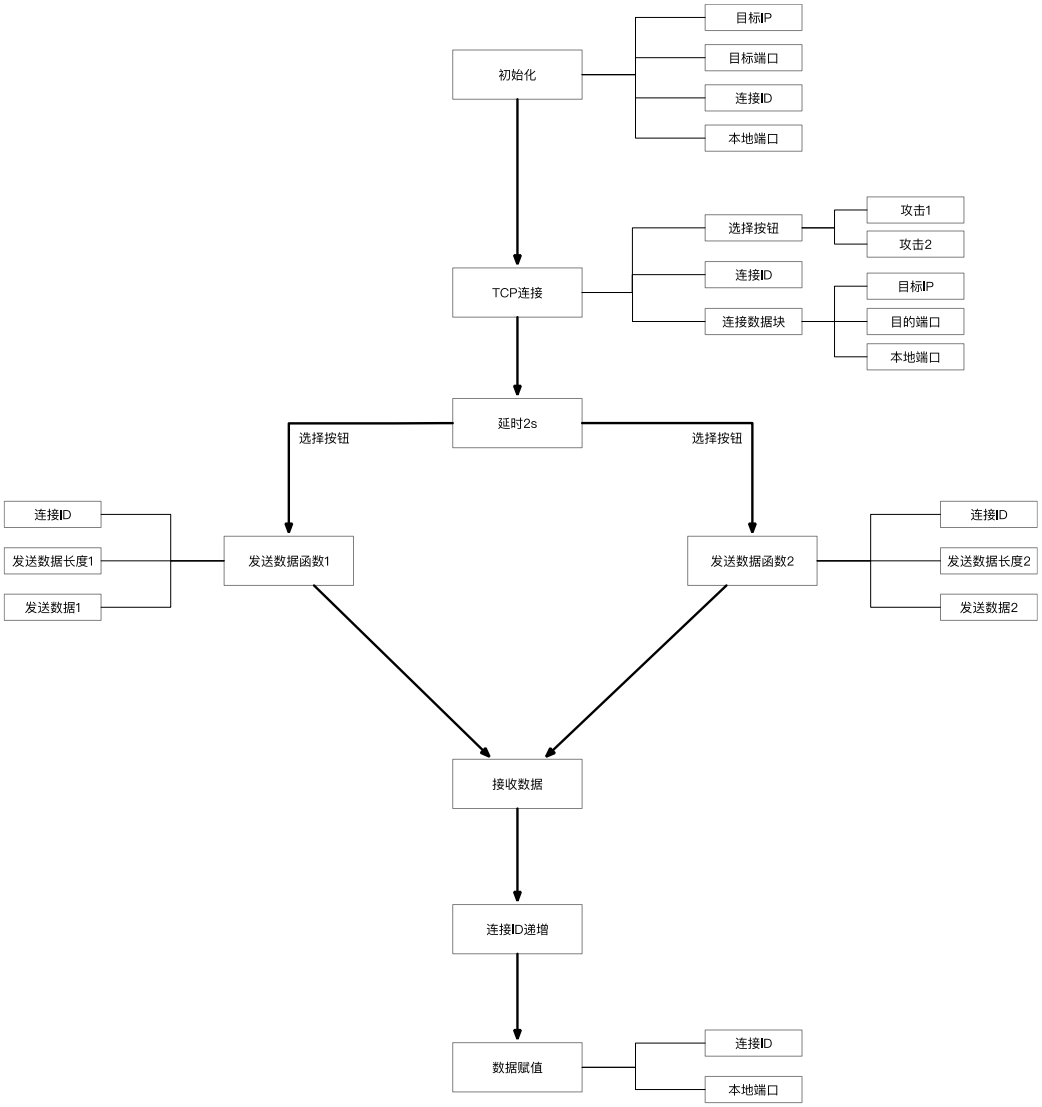


图 1

首先，进行数据初始化。对于网络双方的 IP 信息进行赋值。

其次，调用 PLC 的 TCP 模块进行赋值，将数据、目标 IP 等信息赋值给 TCP 模块。

再次，此处增加了难度，选择了双向可选择发送不同数据的形式，根据自己现场情况，发送不同的攻击代码。

最后，接收返回信息，判断攻击是否成功。并为再次发起攻击做准备。

以西门子博图软件中的以太网模块为例，如图 2 所示。

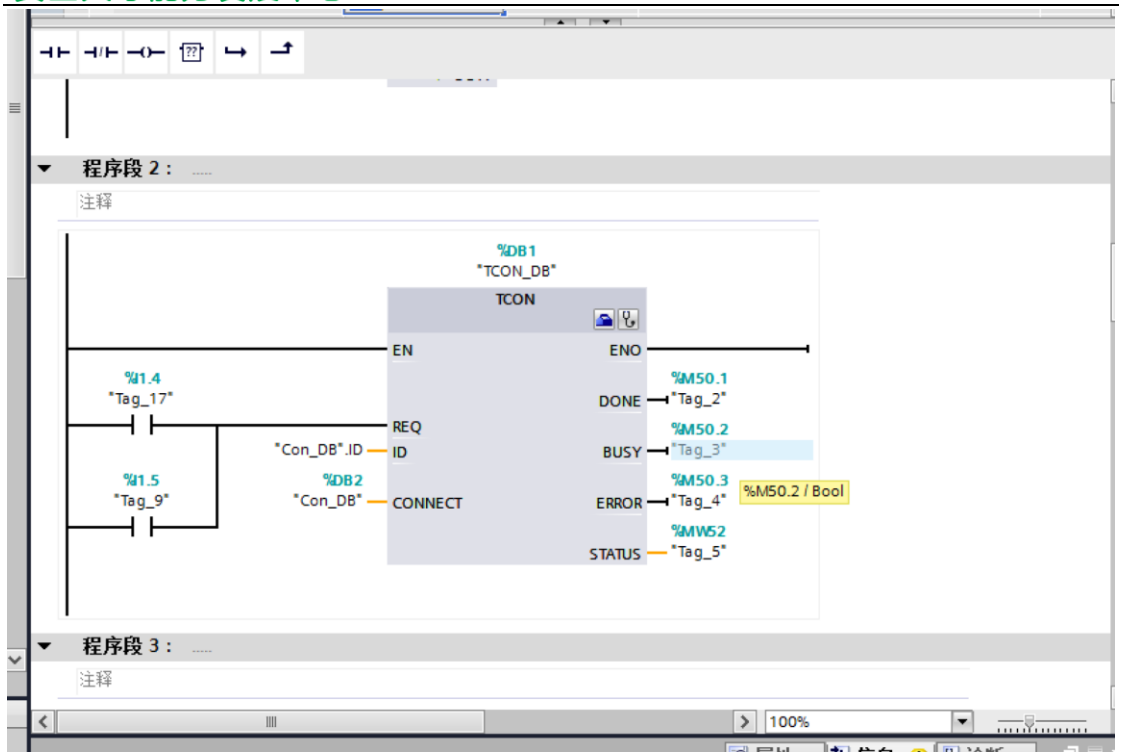


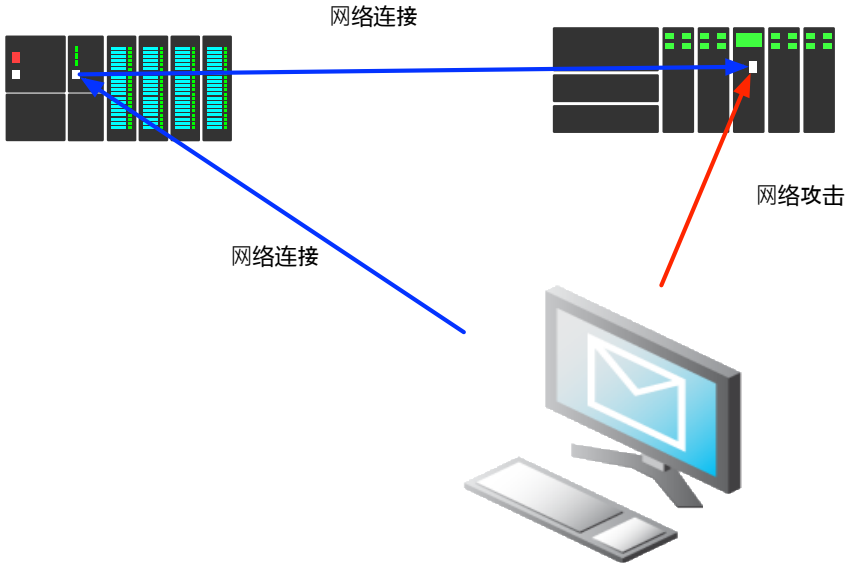
图 2

图 2 中我们主要用到了 TCON 功能模块，该模块是建立 TCP 连接的核心模块。如果我们还想对内网的多个 IP 进行发起攻击，在需要对 CONNECT 参数中的 IP

地址进行及时更换，每次攻击的时候进行目标 IP 地址的切换。

5.2 代理人传播方式

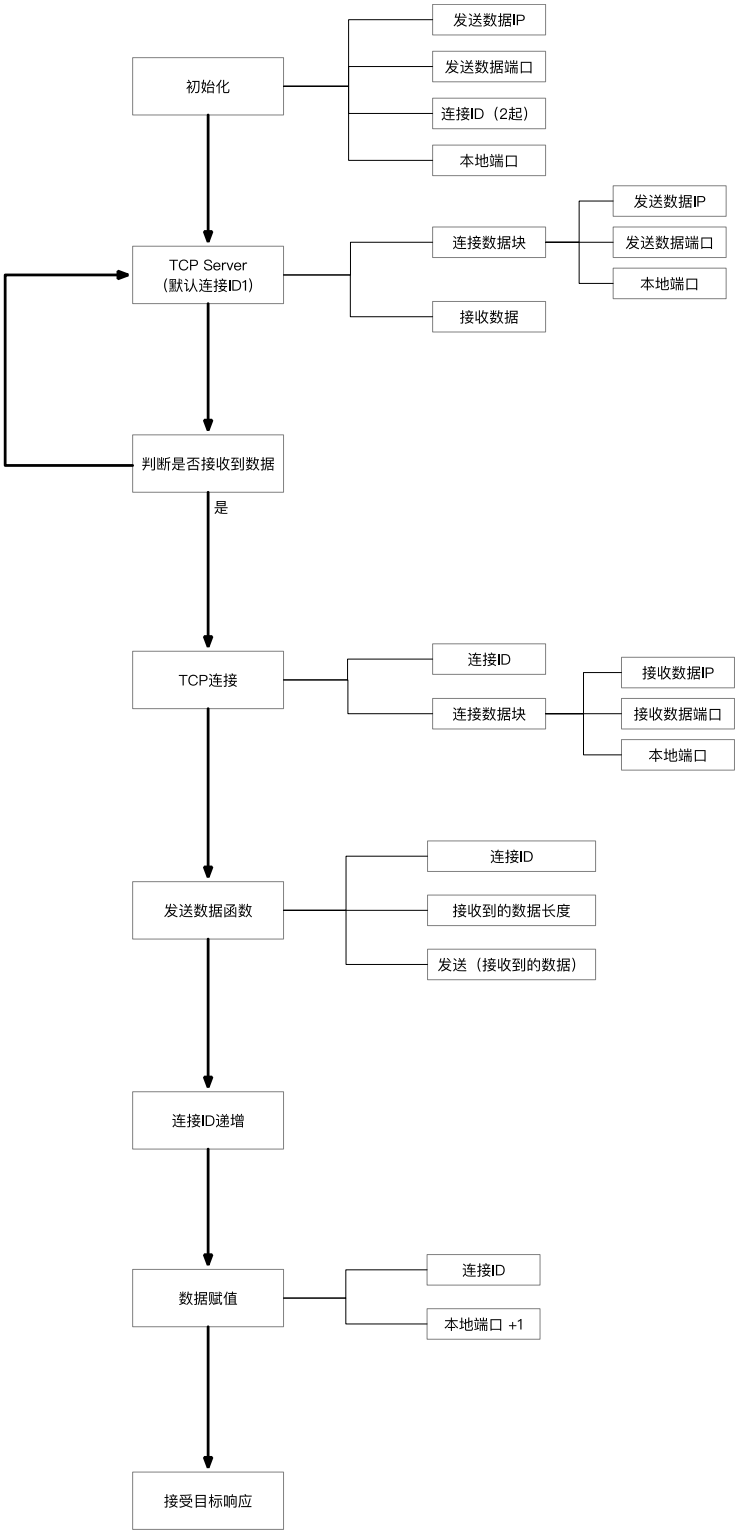
代理人传播方式采用 PLC 代理的形式，间接向目标 PLC 发起网络攻击，网络连接与数据传播如下图所示：



网络连接方式：网络发起者与代理 PLC 直接连接，代理 PLC 与目标 PLC 直接连接。

网络攻击方式：网络发起者攻击目标 PLC。

代理人传播方式的实现逻辑如下图 3 所示：



首先，进行数据初始化。对于网络双方的 IP 信息进行赋值。

其次，代理人 PLC 要进行 TCP Server 参数设置，并启动运行。

再次，代理人 PLC 等待网络发起者发起连接，在网络发起者发起连接后，代理 PLC 会代替网络发起者向目标 PLC 发起网络连接。

发起攻击：网络发起者发送数据，代理人 PLC 会将数据传递给目标 PLC 形成网络攻击的发起。

最后，重置模块，为再次发起网络连接做准备。

以西门子博图软件中的以太网发送模块为例，如图 4 所示。

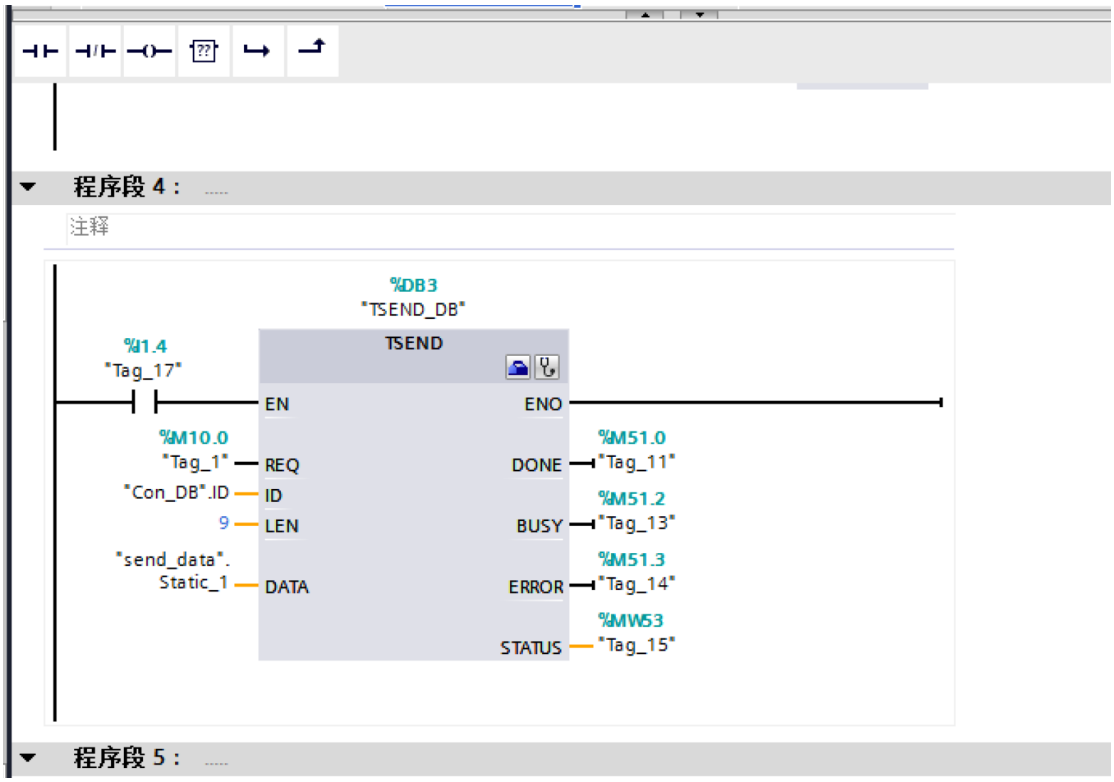


图 4

图 4 中是西门子的 TSEND 的模块，它是将“send_data”数据块中的数据发送出去，以实现通过控制设备对内网其他设备发起网络攻击的目的。

六、 安全防护意见

6.1 网络区域访问控制

将内部网络按照功能进行区域划分，在不同区域间应设置访问控制设备，有效减少因内部网络越权访问造成的网络攻击事件。

6.2 网络安全审计

在内部的核心交换机处，应设置合理的网络安全审计设备，对不明的网络访问加强安全

审计，并及时告警处置。

代理人形式存在这一定的隐蔽性，对于网络数据的综合分析是必须添加的功能。

6.3 协议深度解析防护

在关键的核心设备前端，设置协议深度解析防护设备，对不明的访问请求，功能请求一律进行阻止。防止非法访问造成的设备宕机、工艺错乱等事件。

七、 研究环境介绍

本研究内容是基于 360 工业互联网安全实验箱为基础，进行的工业互联网控制设备攻击方式的研究。其中主要用到了实验箱中的两个目标 PLC 以及电脑主机等设备。整体环境如下图所示：

360 工业互联网安全实验箱是基于模块化的思路在可扩展实验系统进行系统设计，并且支持灵活组网，可以结合应用和上层计算设备采集数据，支持工业互联网平台对接。与教学平台、竞赛平台以及大数据分析平台提供扩展接口。支持工控安全在内的各类自动控制、信息安全、网络安全、协议分析等专项及综合实验。

八、 结语

工业互联网控制设备武器化研究的目的主要为以下几点：

结合当前工业互联网安全事件，判定工业互联网武器化是未来一段时间内的发展方向；

对于控制设备的安全防护手段，仍需要一定技术的突破，以及安全思维的变化；

控制设备是工业生产、工业互联网的基础核心，其网络安全应同步其信息化过程；

控制设备的重点是外联安全，也是大部分安全入侵的入口，外联安全是其网络安全研究方向之一。