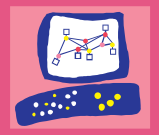


Check Point
SOFTWARE TECHNOLOGIES LTD

SCADA DEMO

How to hack and secure ModBus

Tomas Vobruba | SE Check Point

WELCOME TO THE FUTURE OF
CYBER SECURITY

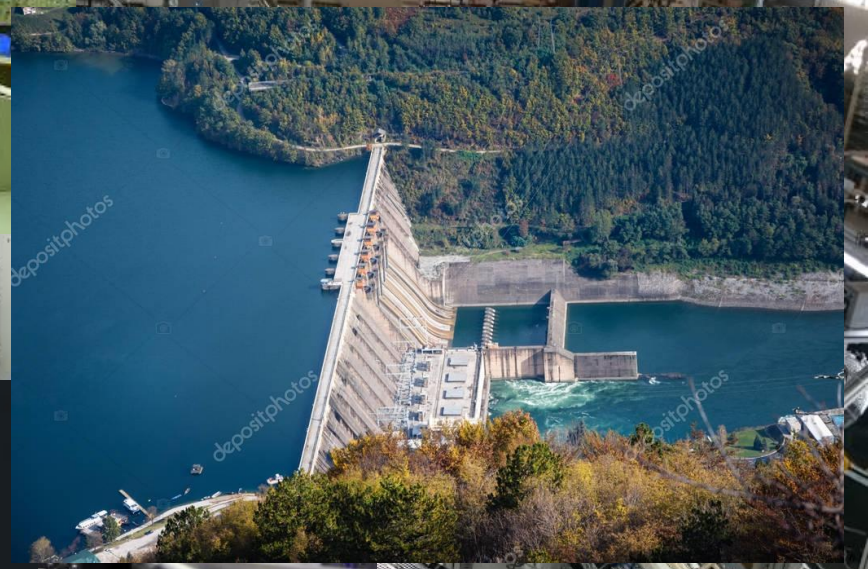
POWERED BY CHECK POINT INFINITY

CLOUD • MOBILE • THREAT PREVENTION




VPKNX
340 - 34
LBE
OAL759
400 - 42
400
AZA473
380 D 37
380
BASUM
AOM818
360 D 35
360
FUA224
380 - 40
380
HLZ
OSN
ROBES
DLE
CFG161
320 - 36
320
GHN231
240 C 37
240
WRB
EDDL
CTN932
122 T 23
GMH
EEDER
EZY130
NOR
VKG115
126 T 38
240



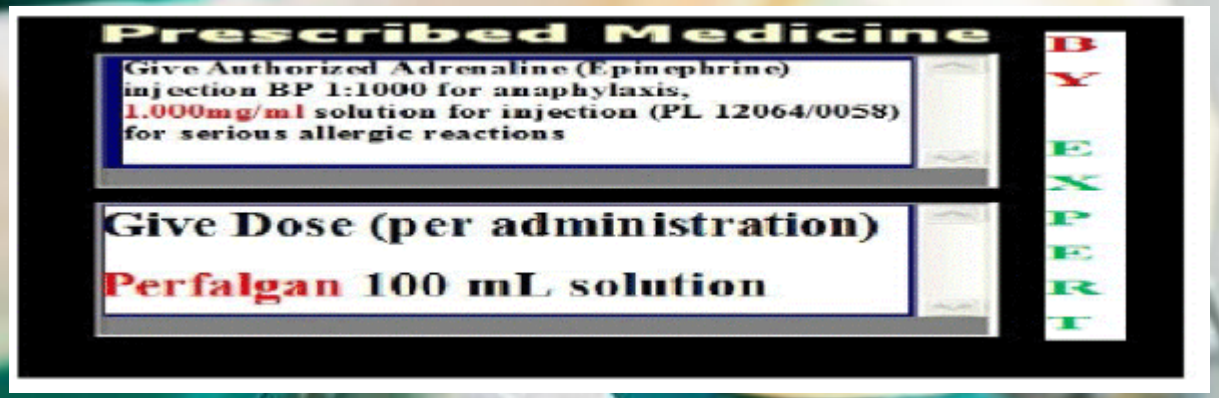









Bohumín



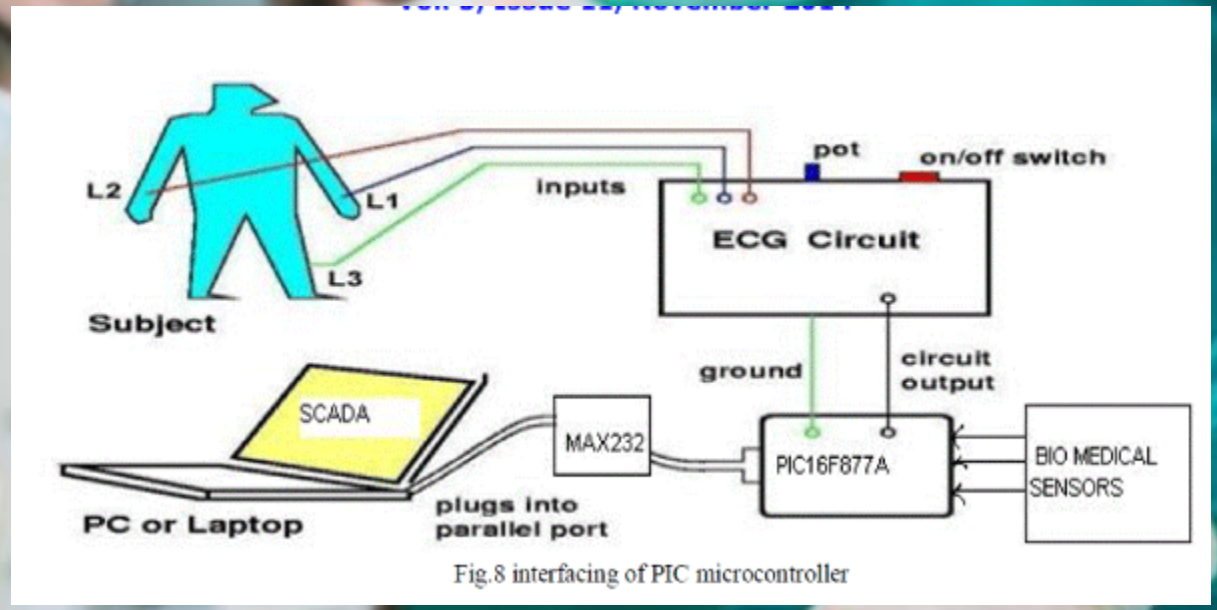


Fig.8 interfacing of PIC microcontroller

Check Point
SOFTWARE TECHNOLOGIES LTD

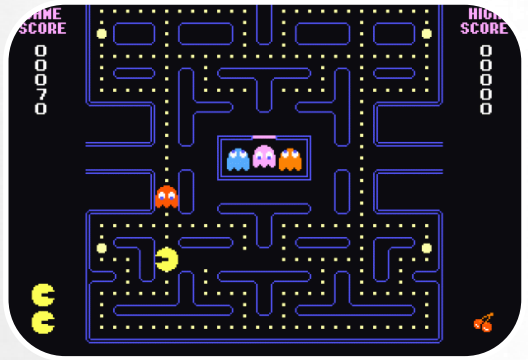
What goes into a Modern Building ??

LonMark | BACnet | OPC | Modbus

Life Safety Systems	Security Systems	BMS Systems	Utility Services
Fire Detection	Access Control	Chiller Management	DG Set Monitoring
Fire Supp (Wet)	CCTV Systems	HVAC Systems	Elevator Control
Fire Supp (Dry)	Intrusion Systems	Ventilation System	Water Leak Systems
VESDA Systems	Perimeter Protection	Energy Metering	Waste Water Management
Paging System	Gate Automation	Lighting Control	Third Party

Schneider

Why Are These Attacks Possible?



Legacy System

Default Configuration

Less/No Updates

Less/No Encryption

Policies & Procedures

Less/No Segmentation

Latency Concerns

Attack Vectors Reaching the OT Network

Removable Media

Email Phishing and Attachments

Remote Technicians

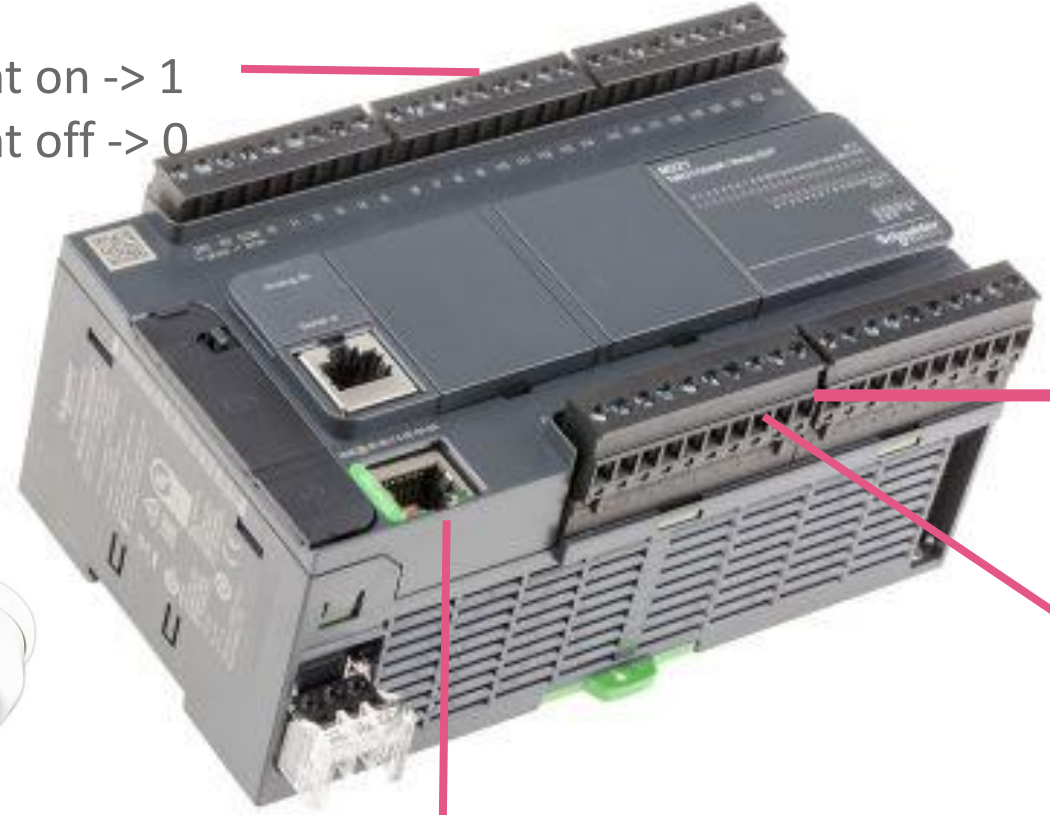
Software Vulnerabilities

Guest Networks Unprotected Sockets

IN:

DC Current on -> 1

DC Current off -> 0

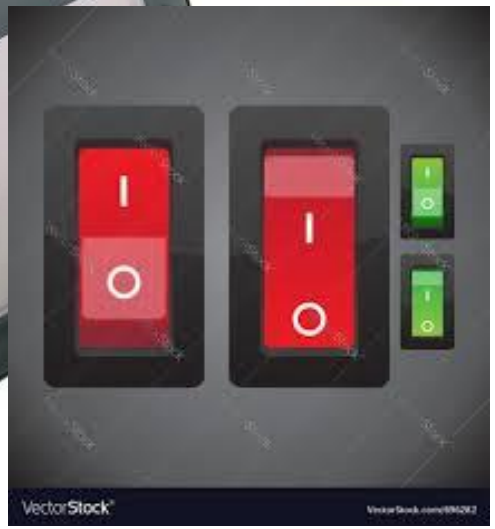


Fire sensor

OUT:

DC Current on -> 1

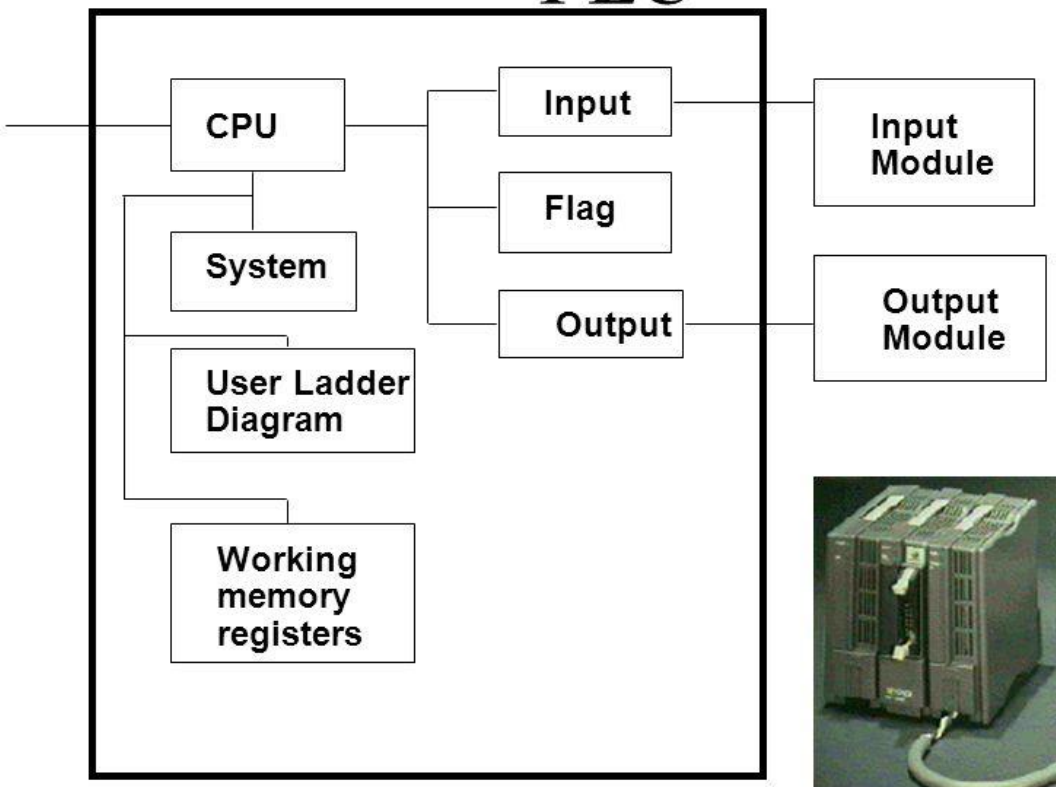
DC Current off -> 0



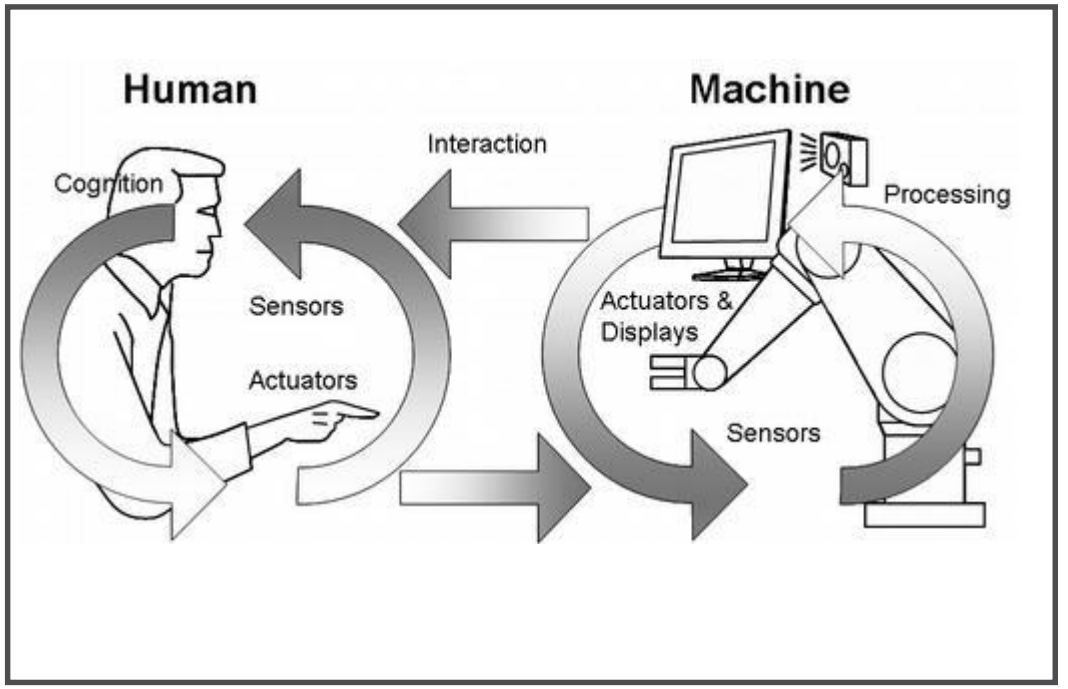
Ethernet

TCP/IP

PLC



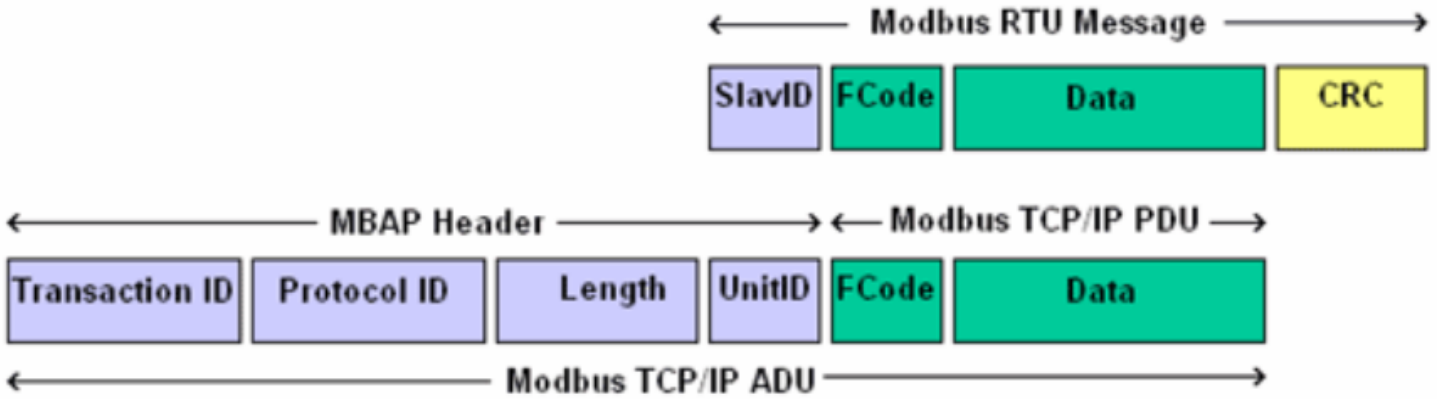
HMI



SCADA Hacking: Modbus

Check Point
SOFTWARE TECHNOLOGIES LTD

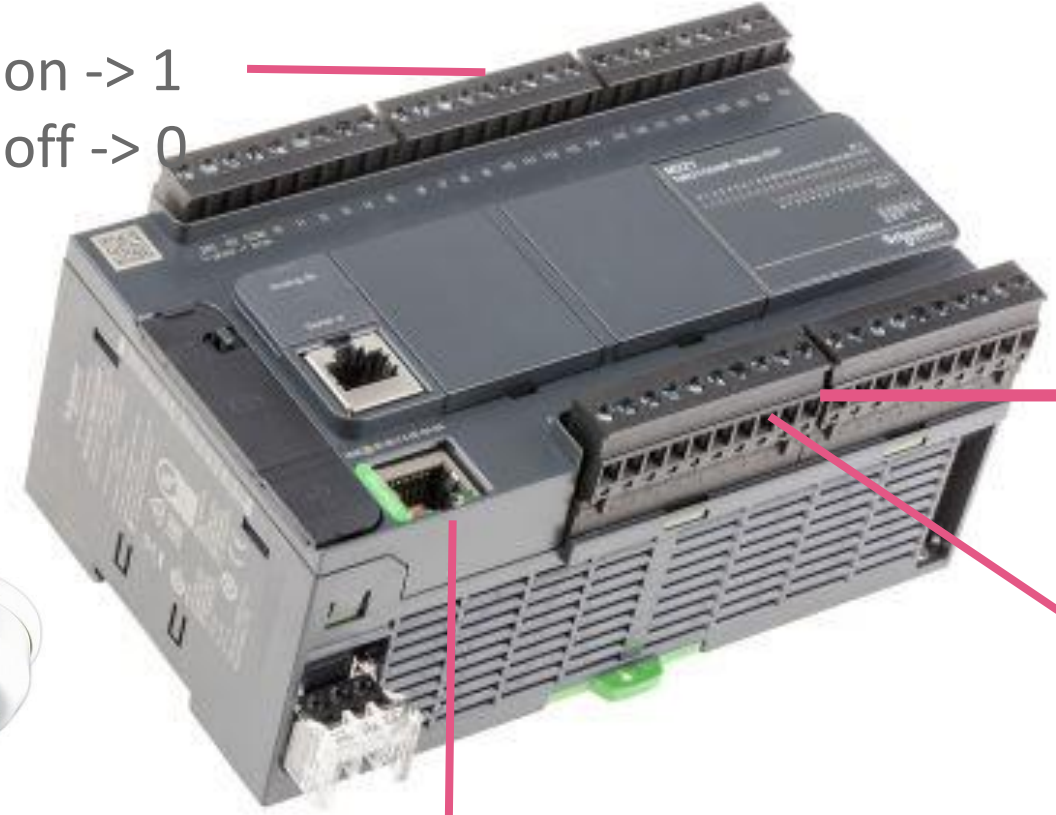
SCADA/ICS systems use many different protocols to communicate than your standard IT systems. The most widely used and the de facto standard is the **modbus** protocol. First developed by Modicon (now Schneider Electric) in 1979 as a serial protocol, it has been modified and updated to run over TCP and is often referred to as **Modbus TCP**. You can see a diagram of the two packet structures below.



Pain

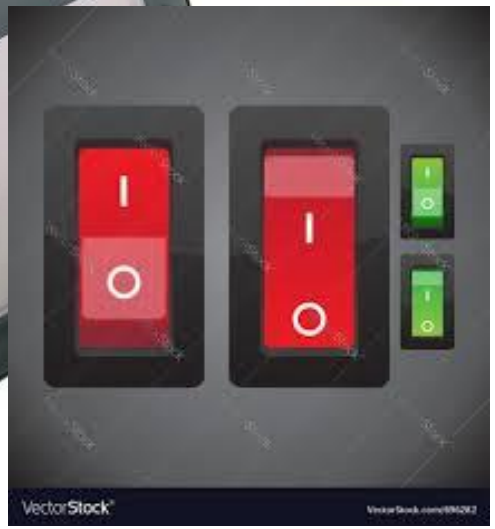
- No security
  - No authentication
  - No authorization
  - No encryption
  - No validation
  - Accessible
  - All open

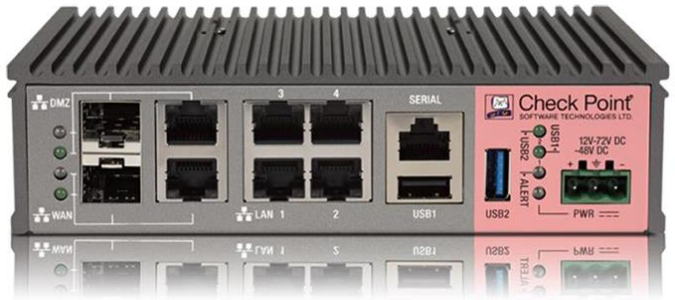
IN:
Current on -> 1
Current off -> 0



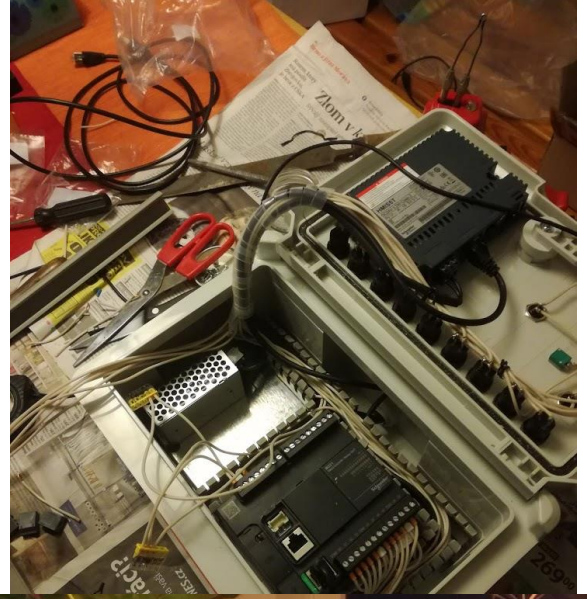
Fire
sensor

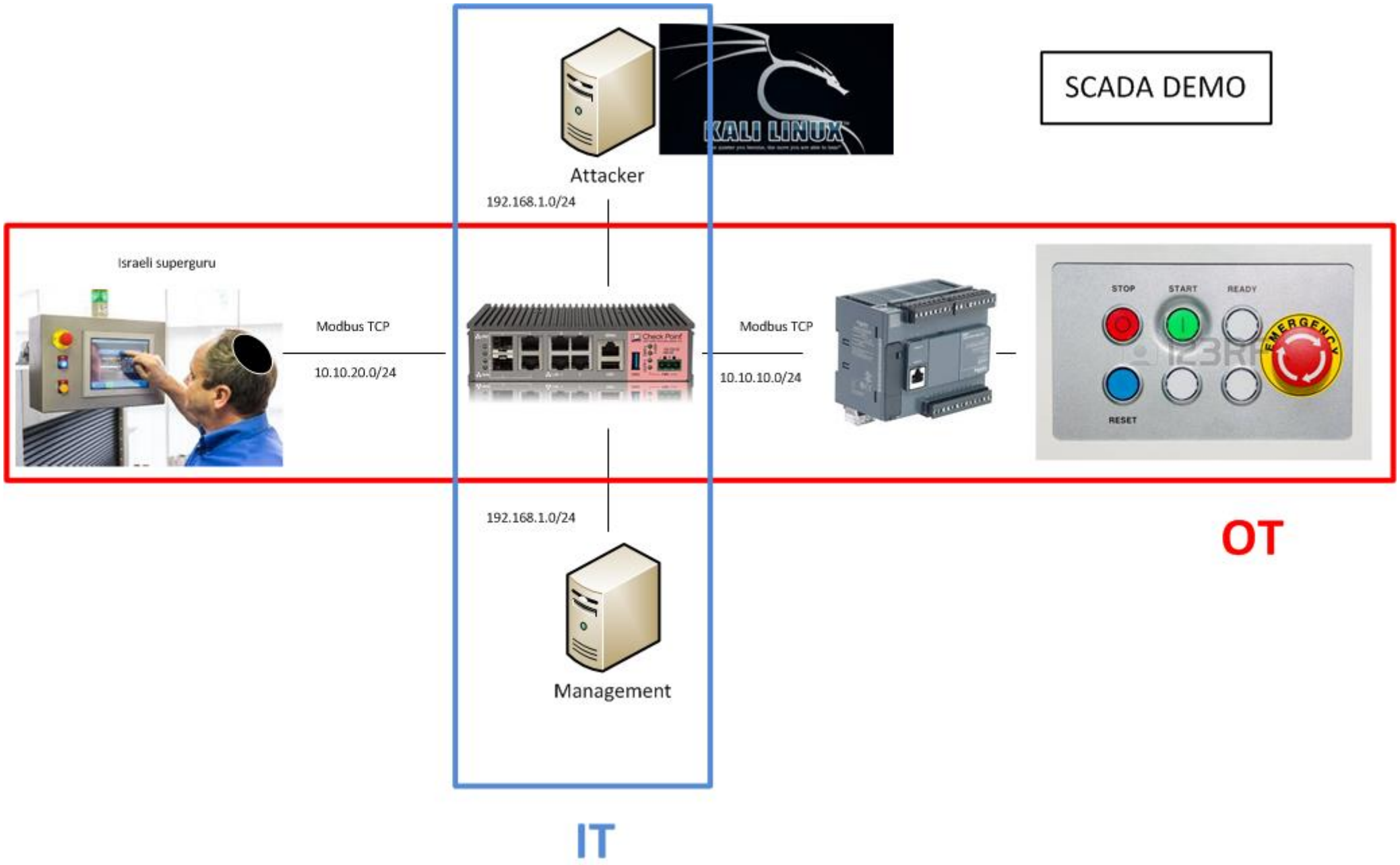
OUT:
Current on -> 1
Current off -> 0





Demo





Check Point
SOFTWARE TECHNOLOGIES LTD

THANK YOU

WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY CHECK POINT INFINITY

CLOUD • MOBILE • THREAT PREVENTION