逆世界：从攻击角度看工控系统防御困境及其应对

信息工程大学 魏强

主要内容

- 一、问题提出：威胁建模分析
- 二、趋势分析：工控漏洞情况
- 二、重点聚焦：PLC安全研究
- 四、防护之难：现实与展望

SCADA之父：物理隔离没什么用

- 2016年6月，Faizel Lakhani
- “电力控制系统在设计过程中从来没有考虑过网络安全。它们的设计目的是管理校准器和电压电流，目前它们的功能也仅限于此。”

- 谁是Faizel Lakhani？
- 20年前，使用一台PDP-11，制造了电站公司历史上的第一个SCADA系统：Ontario Hydro。SCADA技术此后变得无处不在。

Cybersecurity Myths on Power Control Systems: 21 Misconceptions and False Beliefs

IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 26, NO. 1, JANUARY 2011

A.1 "Industrial control systems are isolated"
A.2 "Nobody wants to attack us"
A.3 "We only have obscure protocols /systems"
A.4 "Anti-virus and/or patching are useless for ICSs"
A.5 "Cyber security incidents will not impact operations"
A.6 "Social engineering is not an ICS issue"
B.1 "Our firewall protects us automatically"
B.2 "One-way communication offers 100% protection"
B.3 "It's encrypted: it's protected"
B.4 "Anti-virus protection is sufficient"
C.1 "Obscure protocols/systems are naturally secure"
C.2 "Serial-link/4-20mA wire communications are immune"
C.3 "ICS components do not need to be security hardened"
D.1 "ICS security is a technological problem"
D.2 "It's certified, it's secured"
D.3 "Vendors have a full command of their products security"
D.4 "Compliance with security standards makes you secure"
D.5 "ICS security assessment does not need full inventories"
D.6 "Access points to ICSs are easily controlled"
D.7 "Security is a problem that needs to be solved only once"
D.8 "Cyber security can be handled at the end of the project"

连接世界与被世界连接的问题！

复杂系统设计缺陷（漏洞）不可避免

全球化时代“被后门”不可避免

尚不能实现“泛在彻底”的自主可控

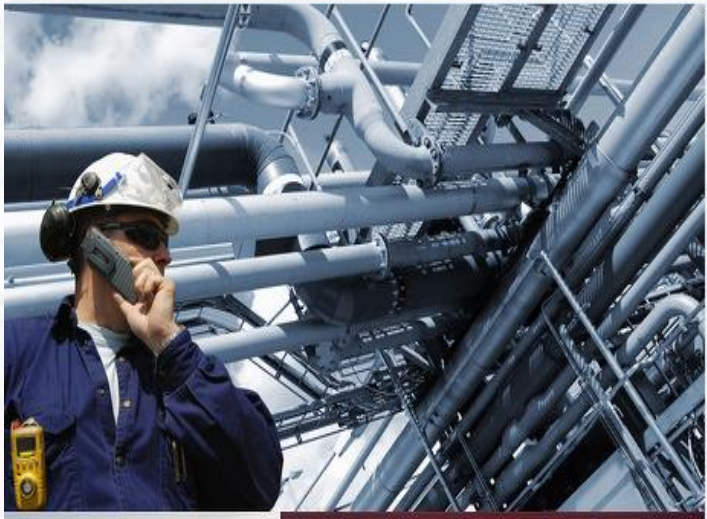
Siemens SIMATIC S7-300 Denial-of-Service Vulnerability

- Advisory (ICSA-16-161-01)
- Original release date: June 09, 2016 | Last revised: June 10, 2016

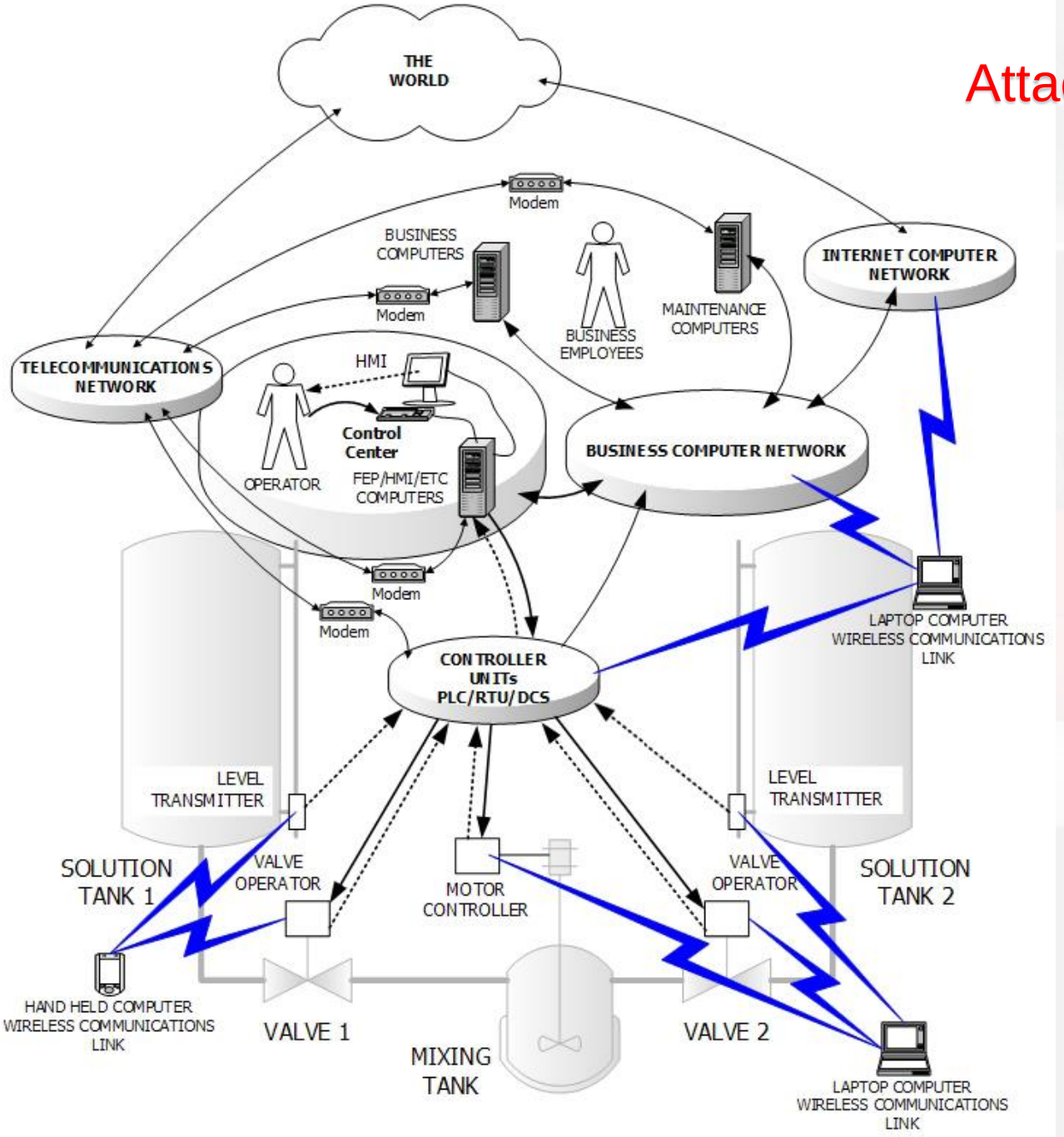
- AFFECTED PRODUCTS
- Siemens reports that the vulnerability affects the following products:
- SIMATIC S7-300 CPUs with Profinet support: All versions prior to V3.2.12, and SIMATIC S7-300 CPUs without Profinet support: All versions prior to V3.3.12.
- IMPACT An exploit of this vulnerability could cause the affected device to go into defect mode, requiring a cold restart to recover the system.

面临的风险威胁

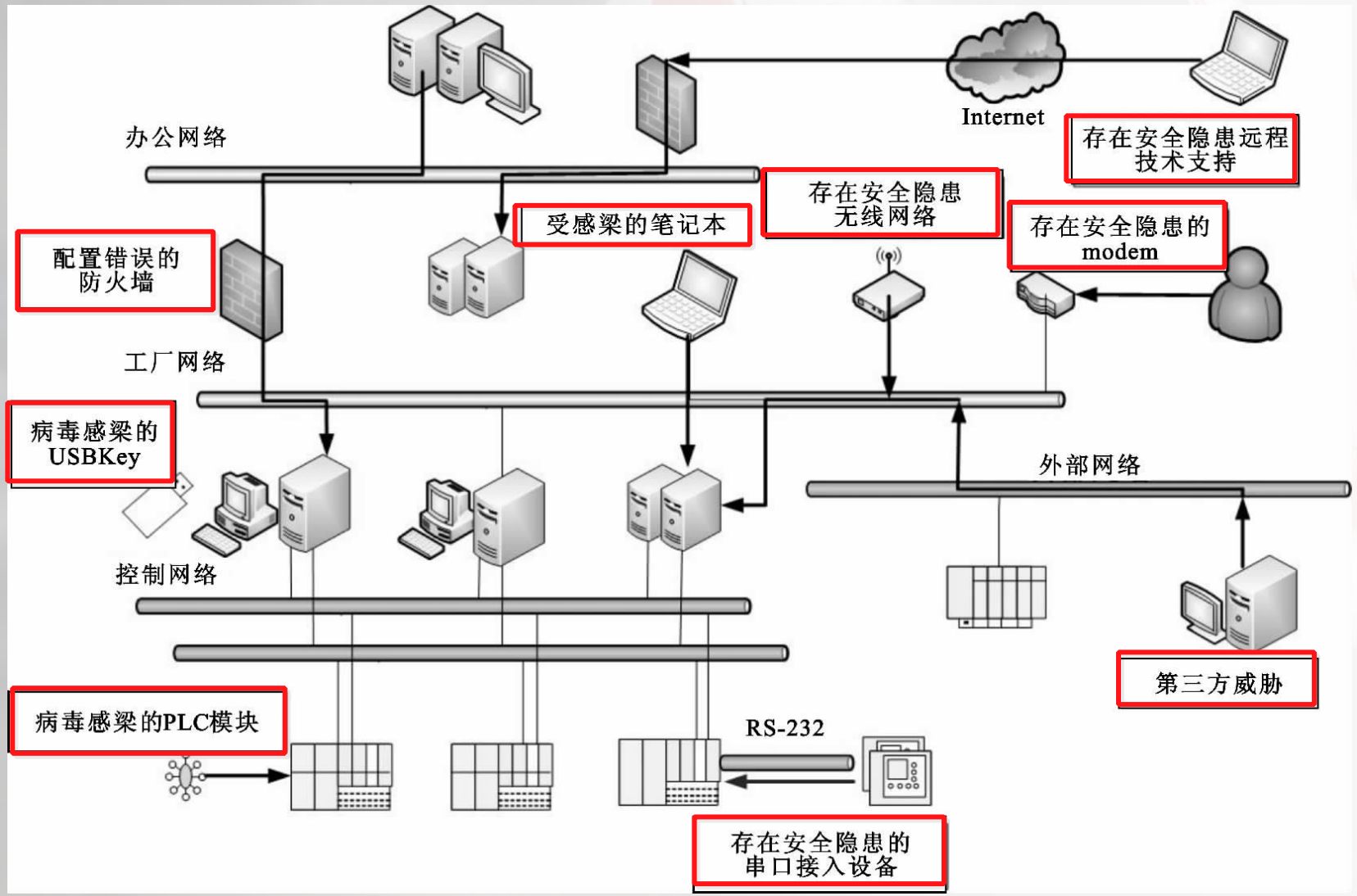
- 两化融合带来的风险
- 采用通用软硬件带来的危害
- 漏洞后门所带来的问题
- 新技术带来的新挑战
- 面对“国家队”威胁



Attack Surface 分析



威胁建模


办公网络
Internet
存在安全隐患远程技术支持
存在安全隐患无线网络
受感染的笔记本
存在安全隐患的modem
配置错误的防火墙
工厂网络
病毒感染的USBKey
外部网络
控制网络
第三方威胁
病毒感染的PLC模块
RS-232
存在安全隐患的串口接入设备

工业控制系统脆弱性分析

脆弱性种类

策略与规程

工业控制系统中不适当的信息安全策略；
人员缺乏ICS 的安全培训与意识培养；
安全流程或流程执行不到位

工控架构

设计缺少信息安全考虑
集中式控制带来的隐患
系统部署复杂，系统、软件更新问题突出
面临威胁来源多（APT）

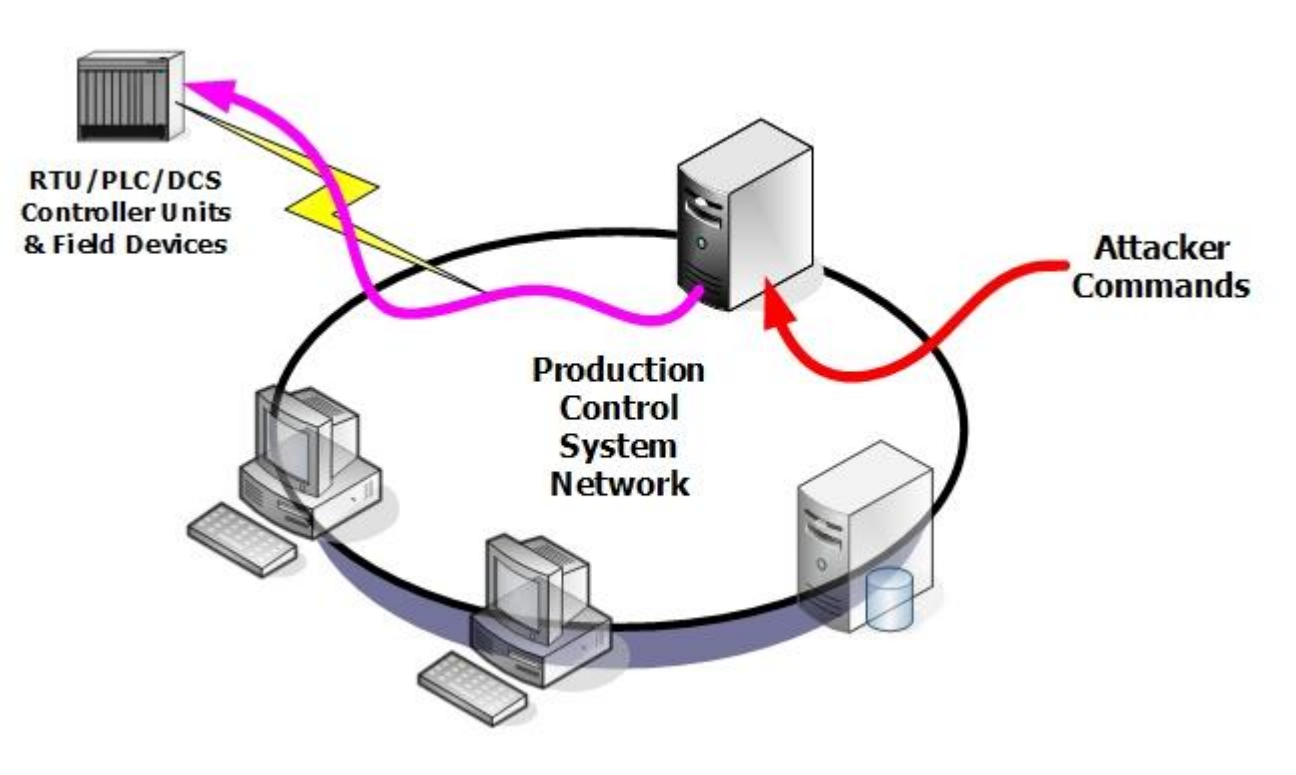
工控平台

平台配置的脆弱性
平台硬件脆弱性
平台软件的脆弱性

工控网络

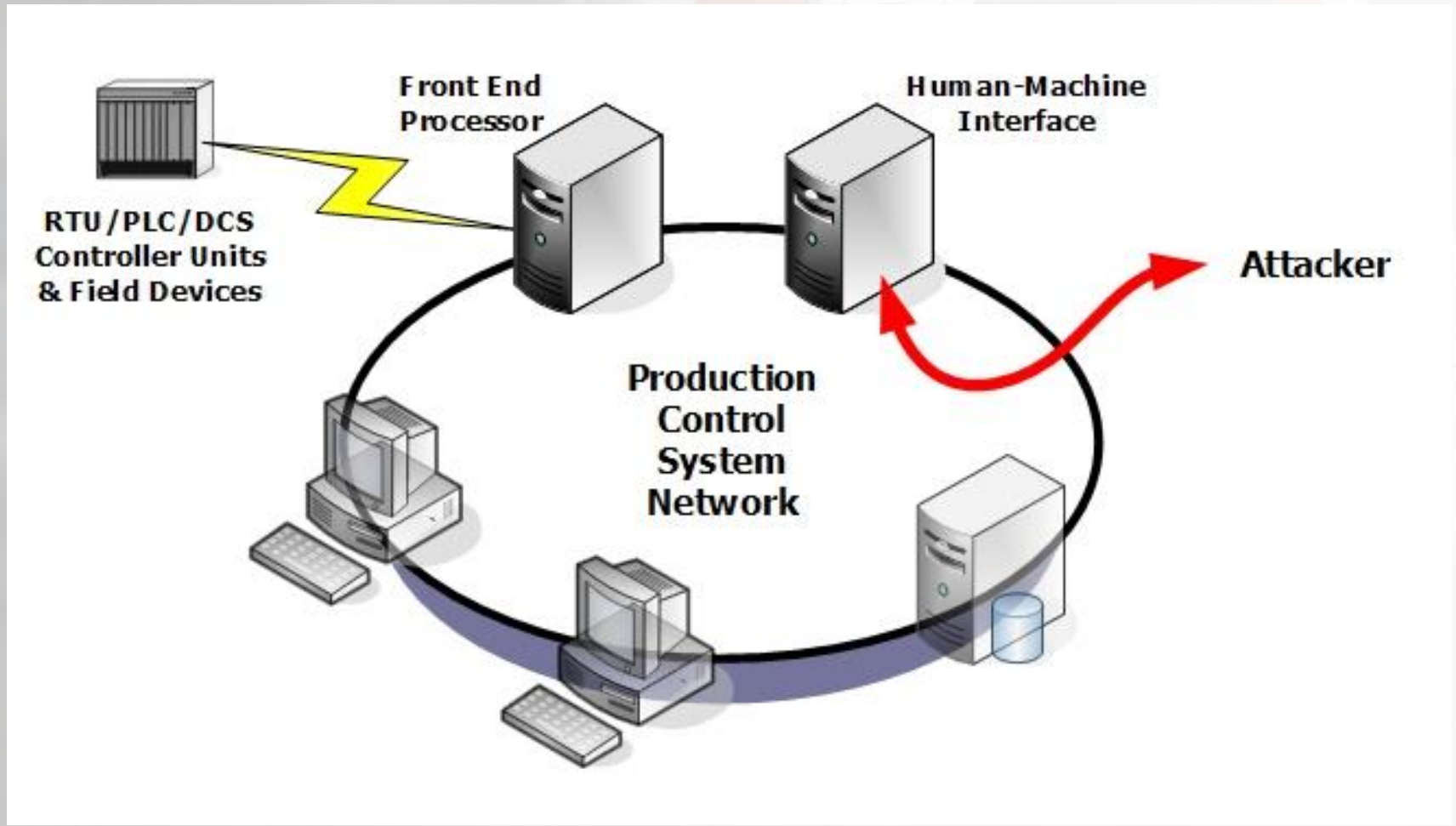
网络配置的脆弱性
网络硬件的脆弱性
网络边界的脆弱性
网络监控与日志的脆弱性

给数据获取设备直接发送命令

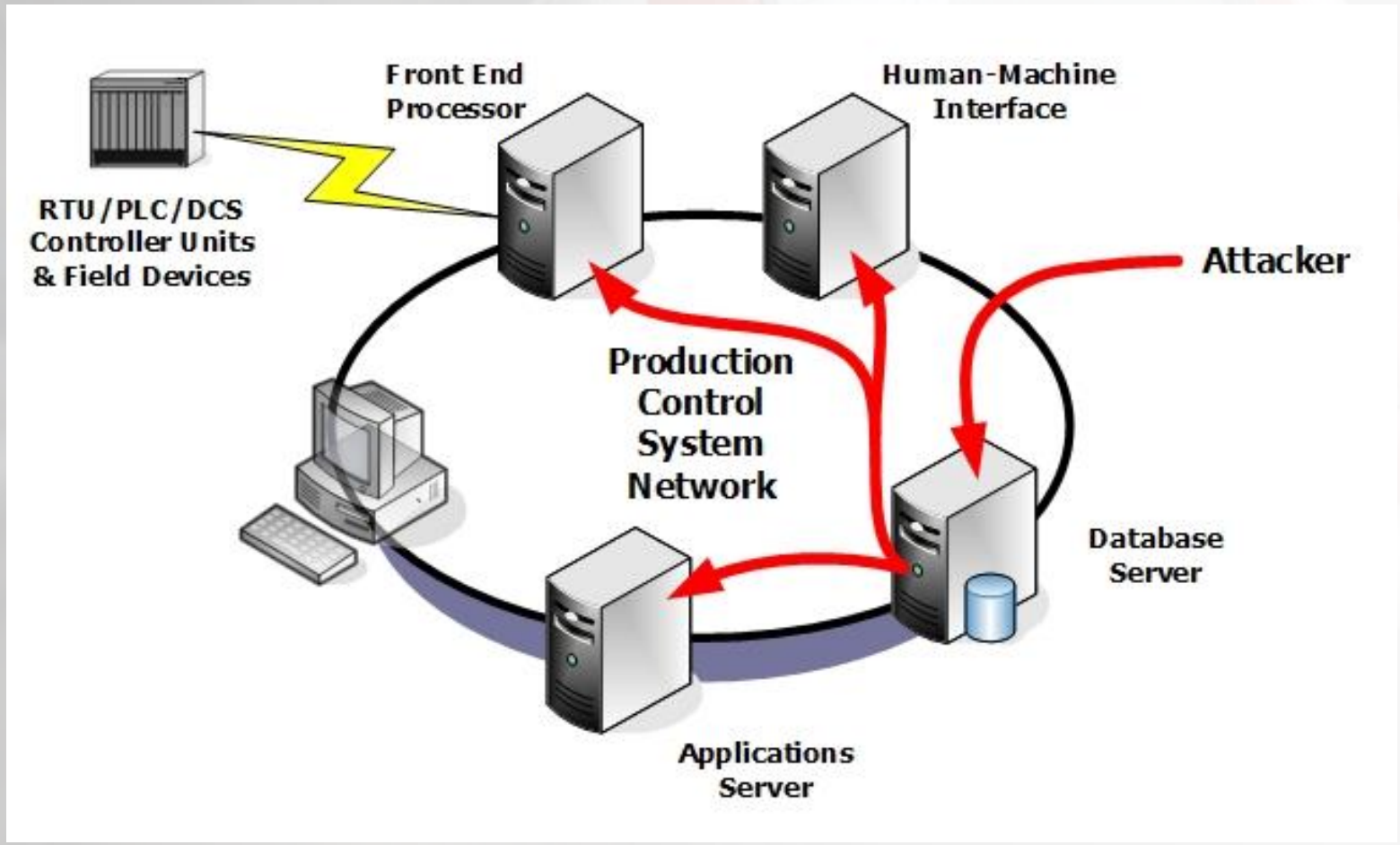


大多数的PLC，协议转换器，数据获取服务器缺乏最基本的认证。

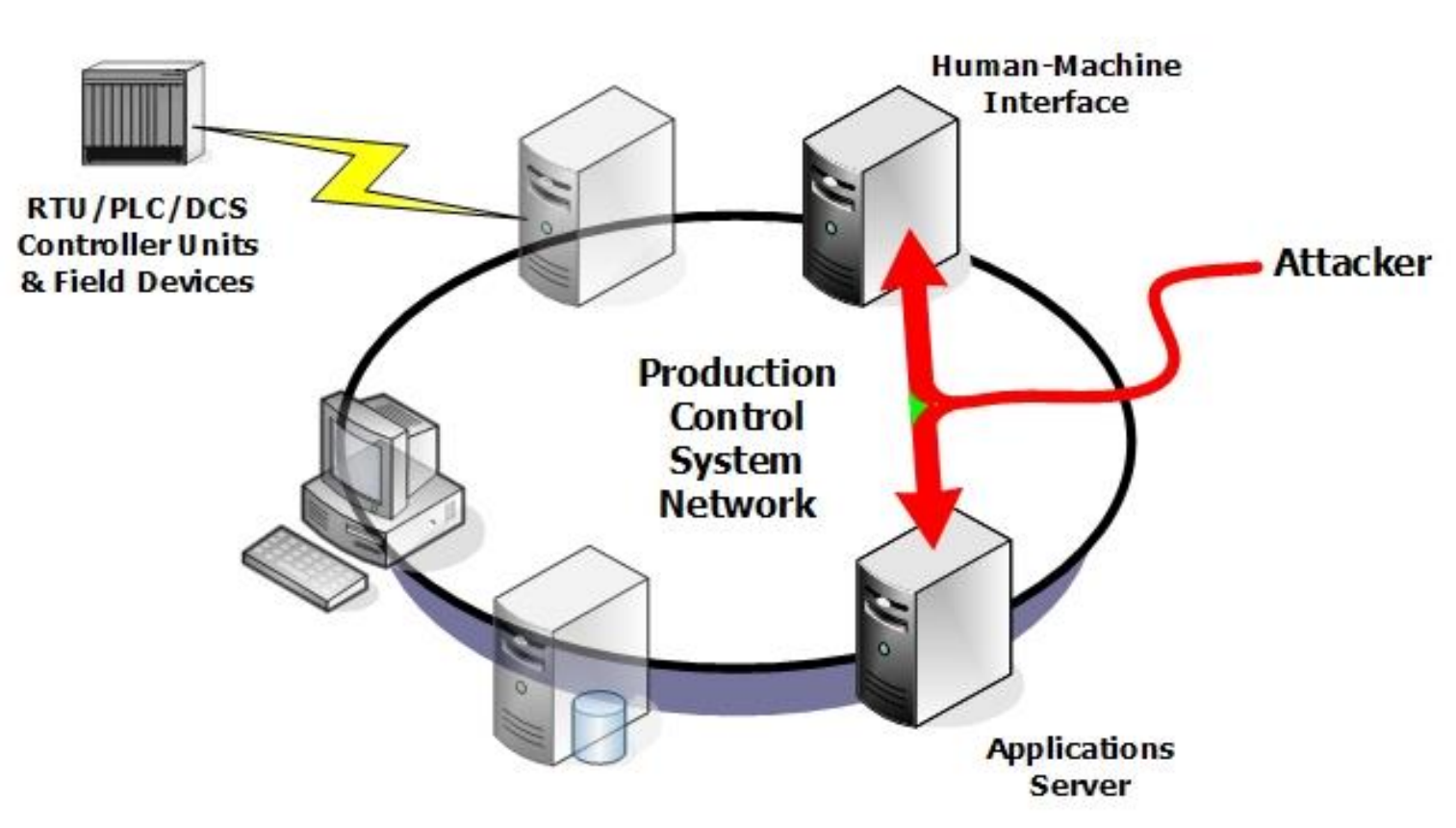
导出HMI屏幕


Front End
Processor
Human-Machine
Interface
RTU/PLC/DCS
Controller Units
& Field Devices
Attacker
Production
Control
System
Network

改变Database


Front End
Processor
Human-Machine
Interface
RTU/PLC/DCS
Controller Units
& Field Devices
Attacker
Production
Control
System
Network
Database
Server
Applications
Server

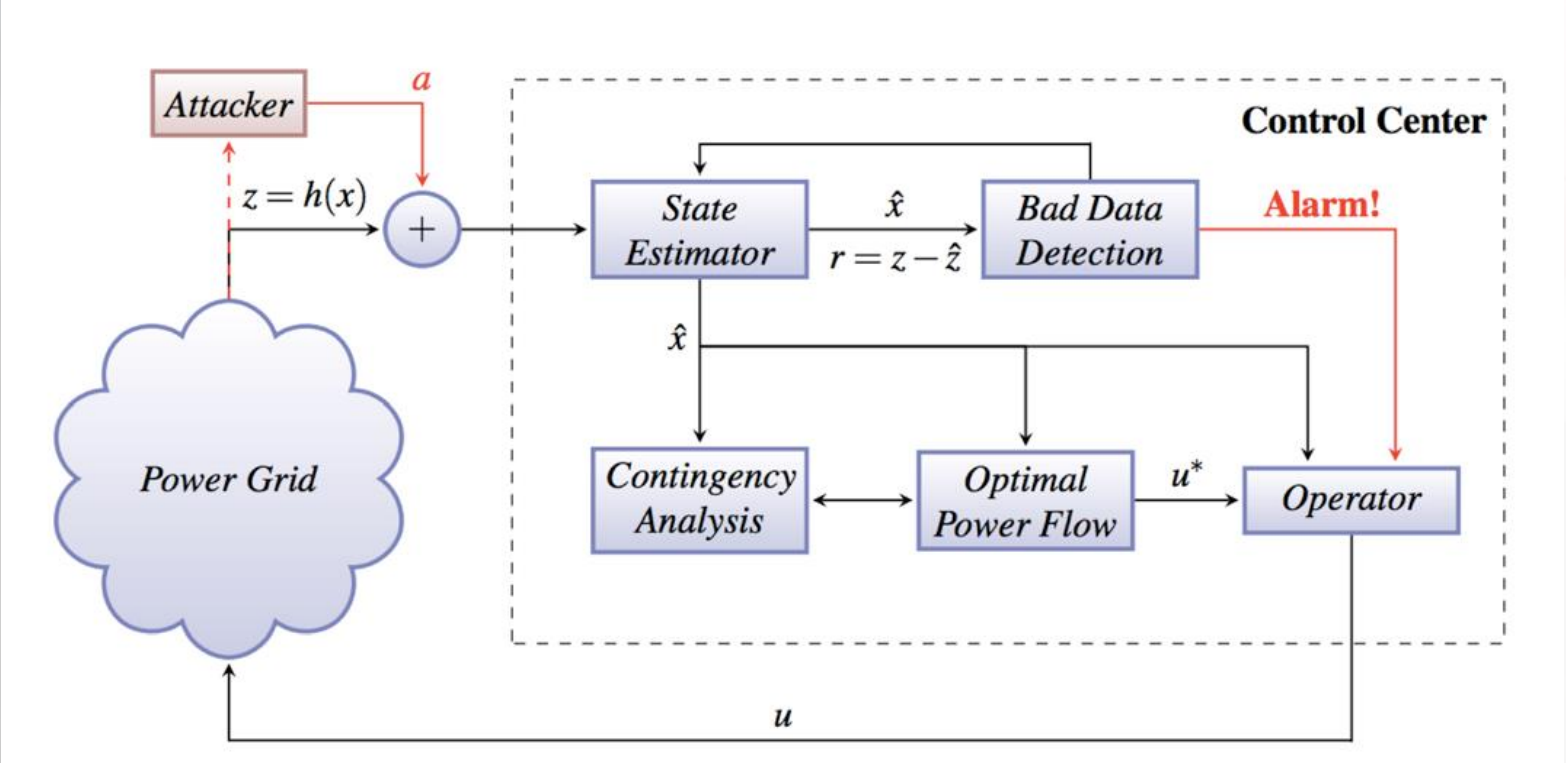
Man-in-the-Middle Attacks



通过插入命令到命令流里来导致任意或者目标命令执行

False data injection

- 以Power Grid为例：
  - 伪造测量数据
  - 避免被检测为“坏”数据
  - 误导控制器



概念验证病毒

- PLC-Blaster: A Worm Living Solely in the PLC

Target discovery

– Portscanner (TCP 102); TCON, DISCON

● Carrier

– Implement the S7-Protocol; TSEND, TRCV

● Activation

– Built-in

● Payloads

– A lot of possibilities

Memory usage

– 38,5kb RAM

– 216,6kb persistent memory

Model RAM Persistent Memory

S7-1211 50kb (77%) 1Mb (21%)

S7-1212 75kb (51%) 1MB (5 %)

S7-1214 100kb (38%) 4MB (5 %)

S7-1215 125kb (30%) 4MB (5 %)

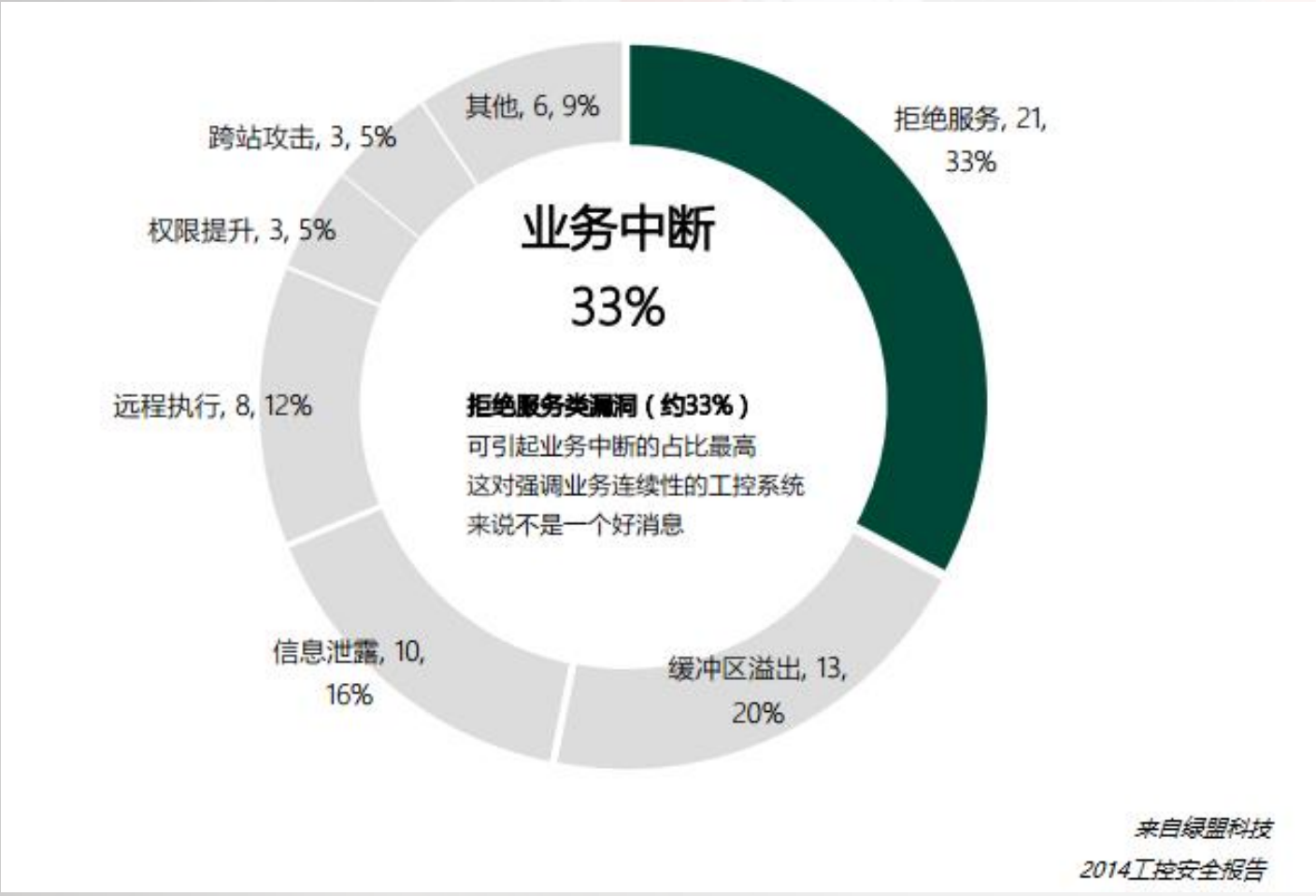
S7-1217 150kb (25%) 4MB (5 %)

二、焦点问题：工控系统漏洞

- 在CVE的7w多漏洞，涉及工控系统漏洞在400以上，其中西门子、施耐德的漏洞超过了总数的50%

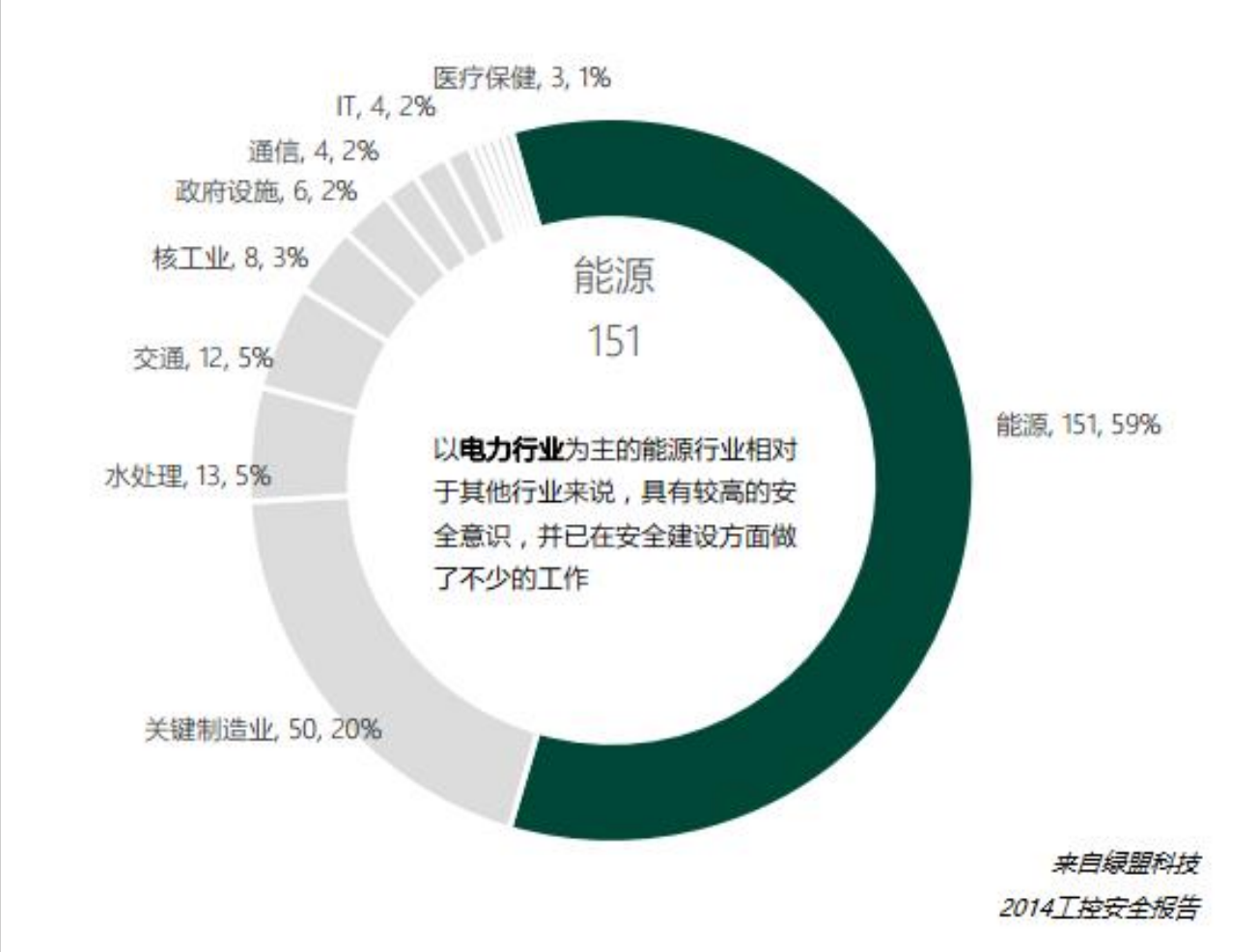
- BlackHat, S. Bratus, “Fuzzing proprietary SCADA protocols,” presented at the Slides presented at the Black Hat USA Conf., Las Vegas, NV, Aug.2008
- M. Bristow, “ModScan: a SCADA Modbus network scanner,” presented at the DefCon-16 Conf., Las Vegas, NV, 2008, slides presented
- D. Goodin, “Gas refineries at Defcon 1 as SCADA exploit goes wild—At least they should be.,” The Register, Sep. 2008.
- B ERESFORD, D. Exploiting Siemens Simatic S7 PLCs. In Black Hat USA (2011).

工控事件所涉及的重要行业及分布

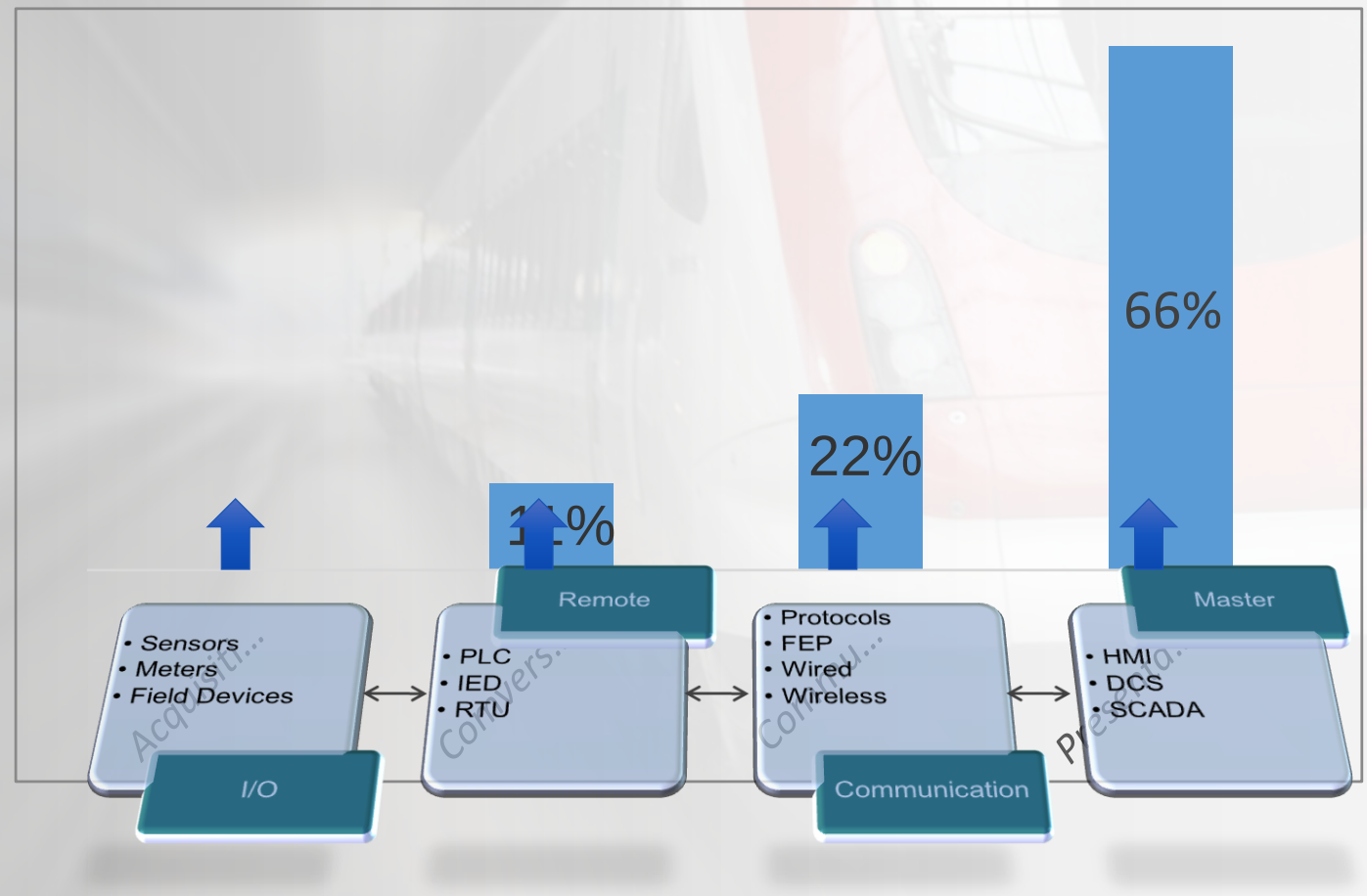


来自绿盟科技
2014工控安全报告

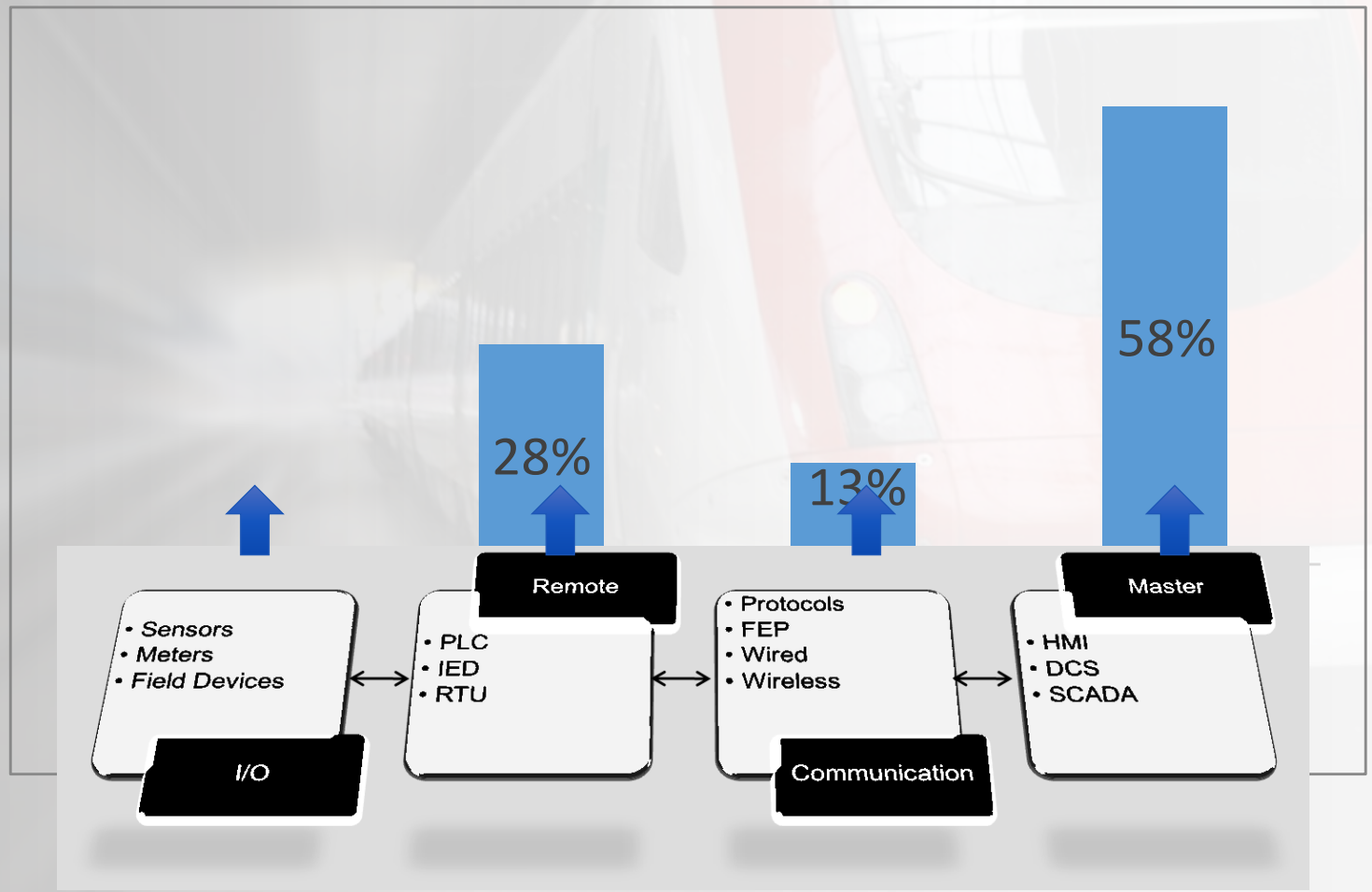
2014年新增漏洞威胁分类及占用比分析



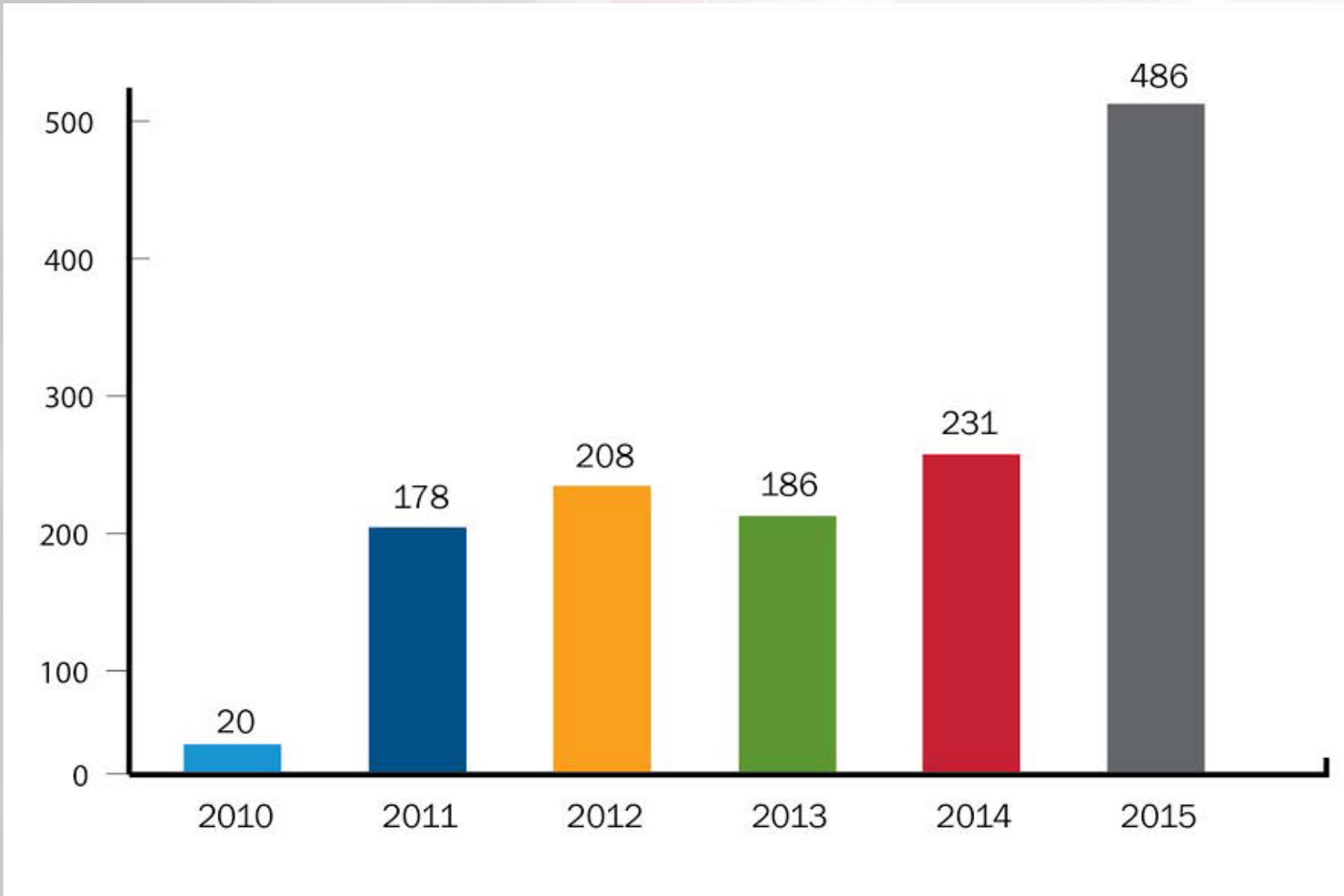
2013年工控漏洞分类统计



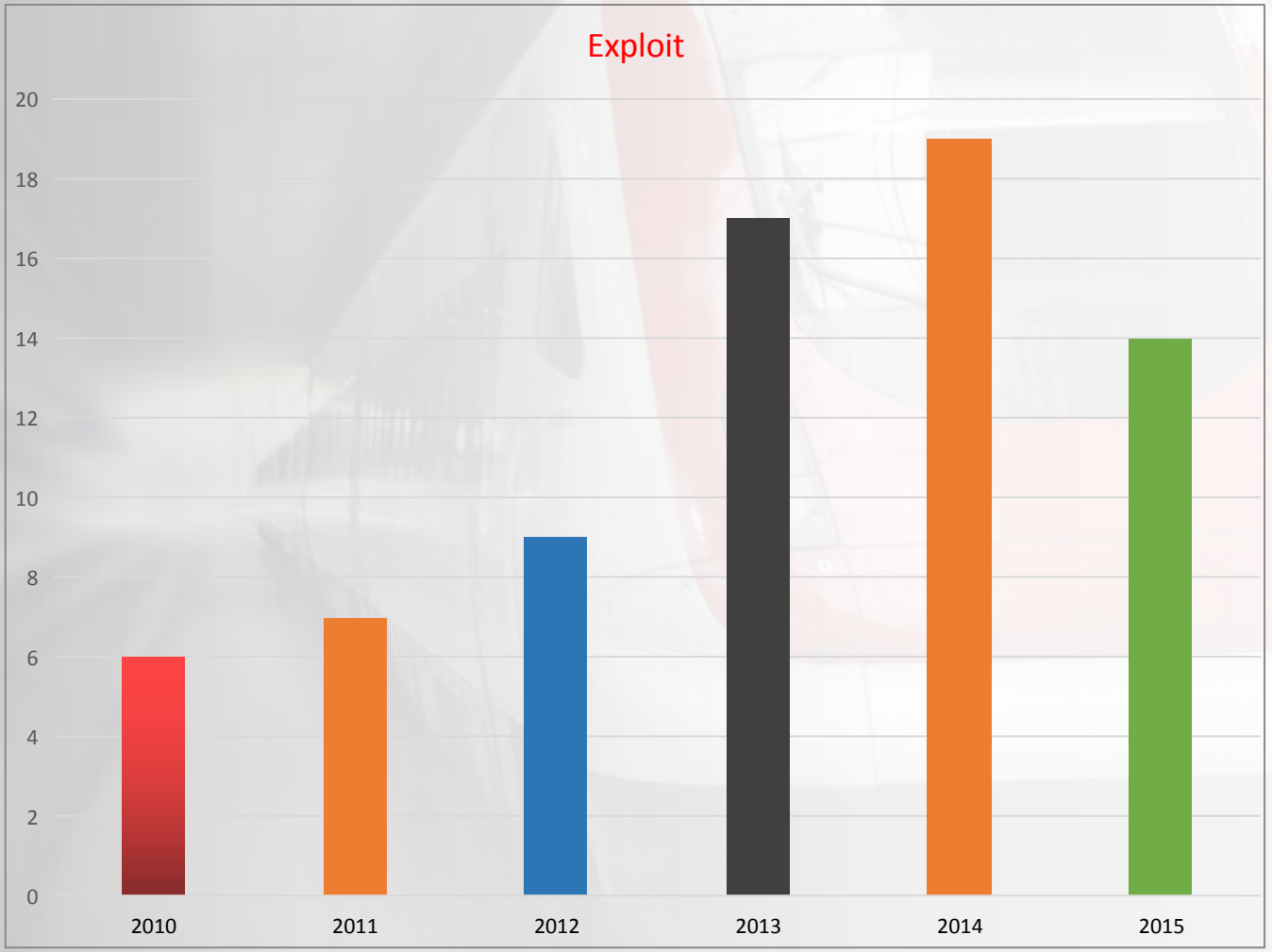
2014年工控漏洞分类统计

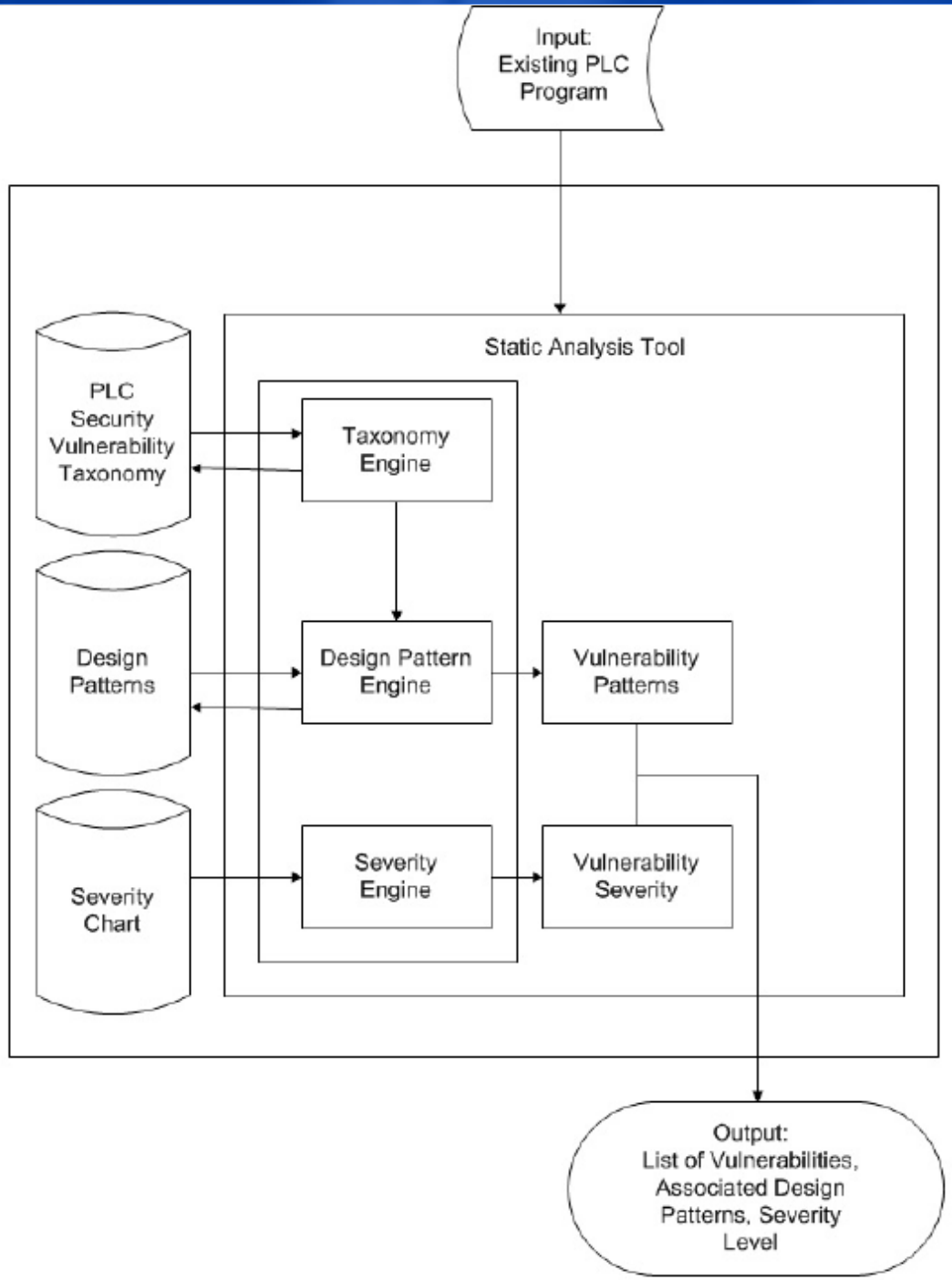


漏洞数量


500
400
300
200
100
0
20
178
208
186
231
486
2010
2011
2012
2013
2014
2015

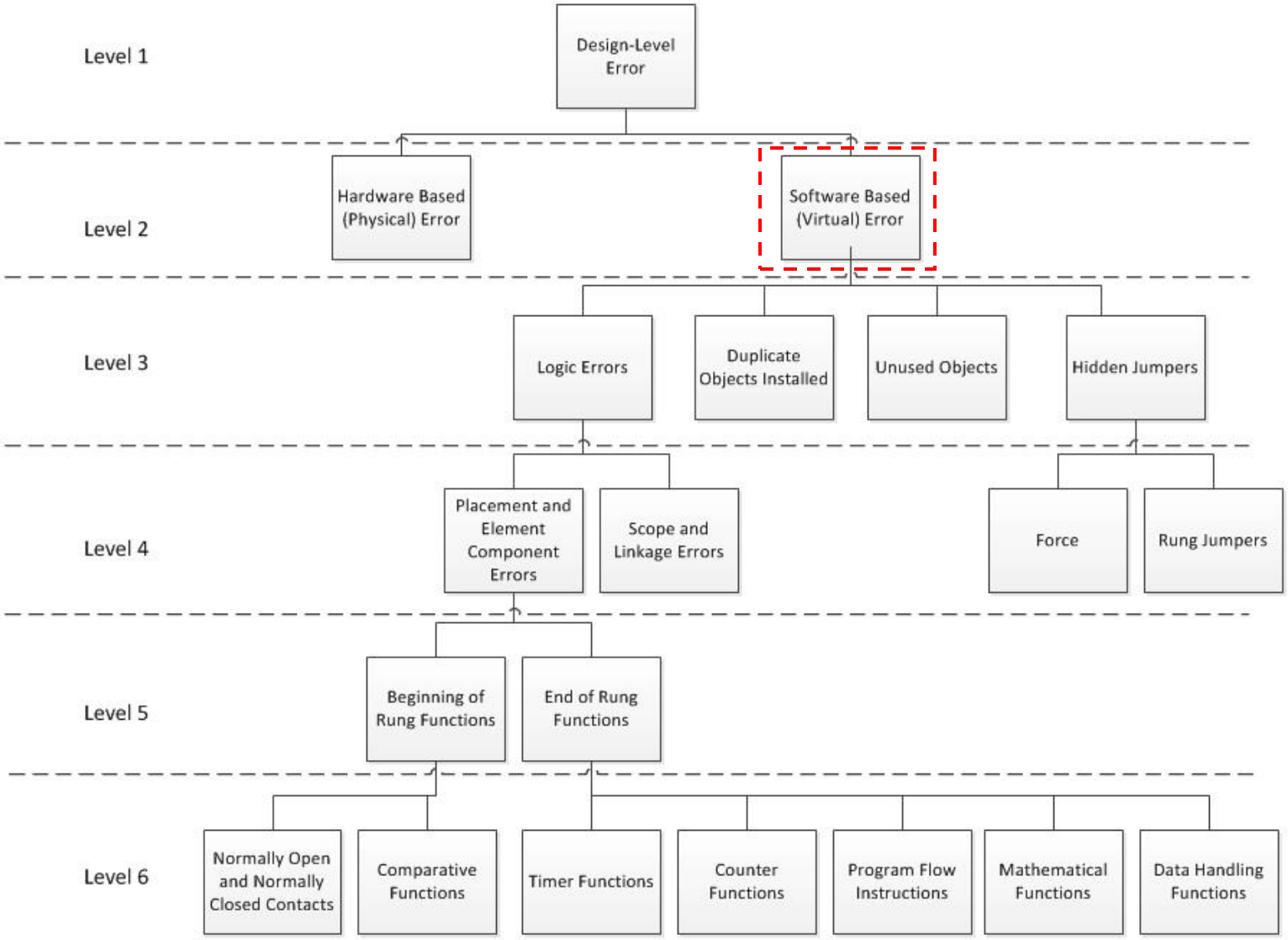
漏洞利用代码数量



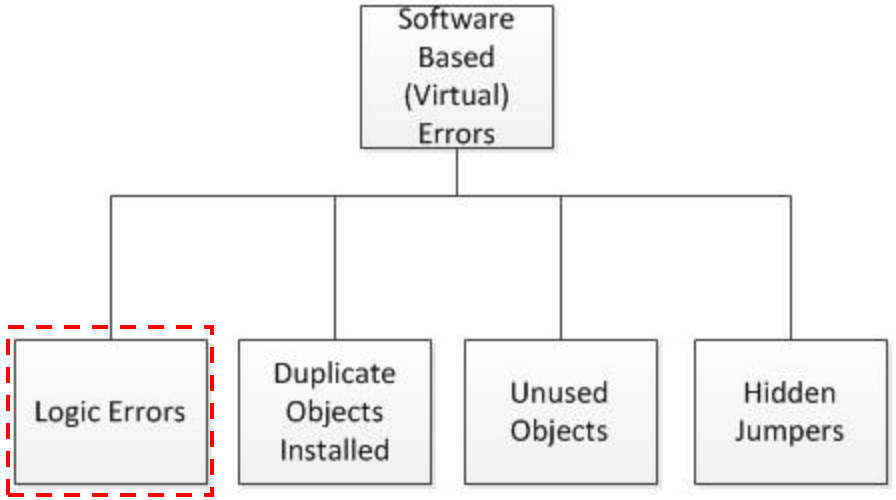


PLC Code Vulnerabilities Through SCADA Systems，Sidney E. Valentine, Jr. 南加州大学，2013

Building the Vulnerability Taxonomy



Building the Vulnerability Taxonomy

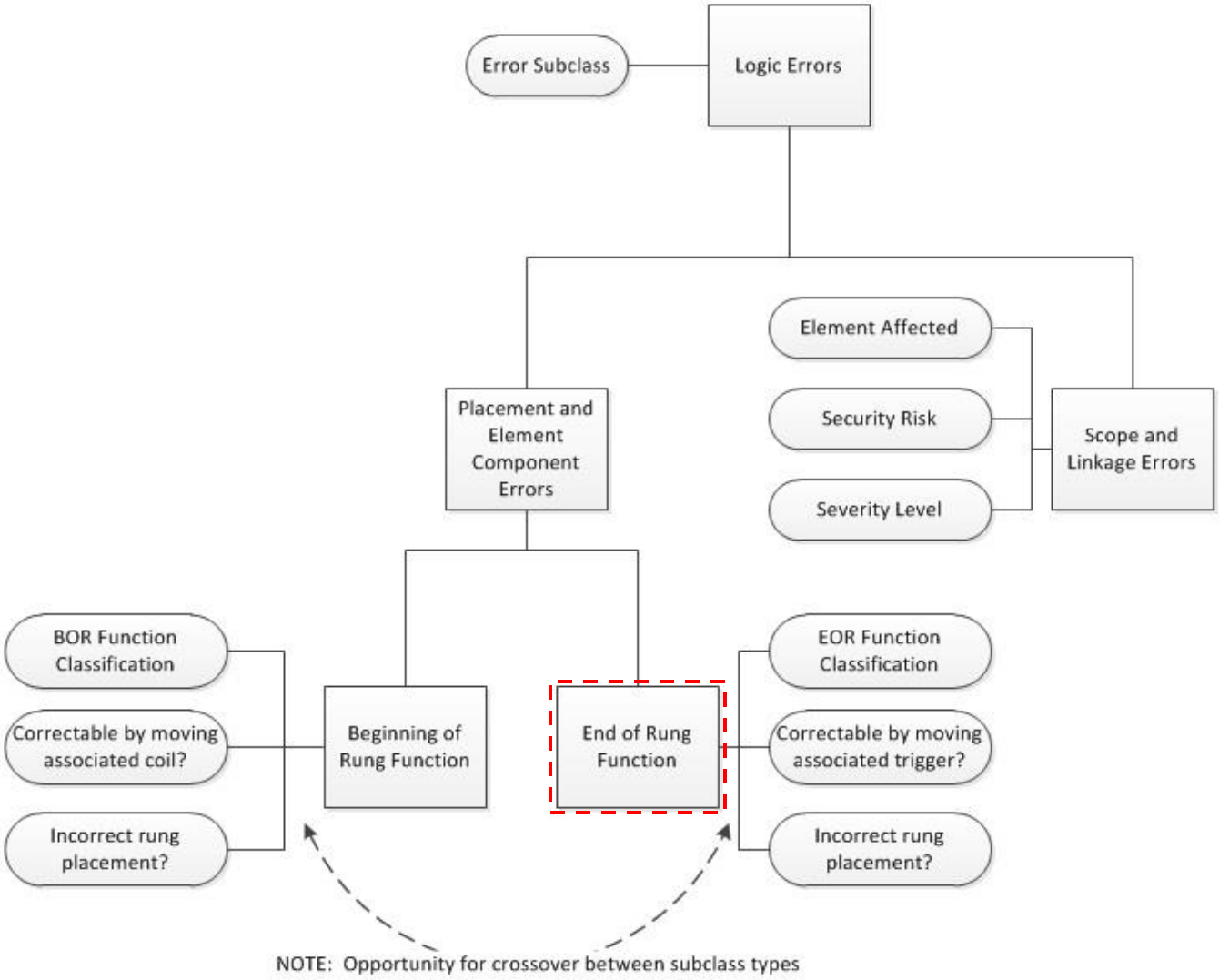


多次定义的对象，例如：线圈、定时器、计数器等

在初始数据库中定义，但在梯形图逻辑中从未使用

Vulnerability Taxonomy: Software Based (Virtual) Errors

Building the Vulnerability Taxonomy



从2013和2014年工控漏洞事件分类统计来看，公开漏洞中以SCADA/HMI系统相关的漏洞最多，其占比超过了1/2。

其中工控漏洞事件中，包括可编程逻辑控制器（PLC），智能电子设备（IED）的漏洞事件比重有所上升，由13年的11%上升到14年的28%,其中引起该占用比上升的主要原因是可编程逻辑控制器（PLC）新增漏洞数量的增加。

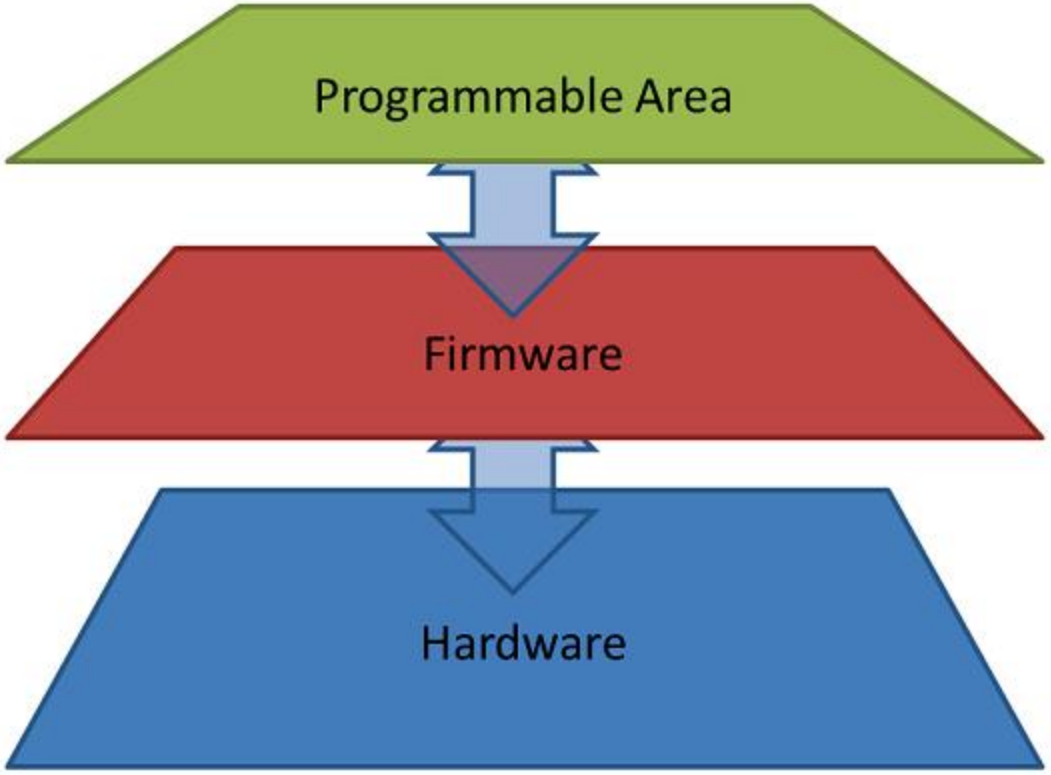
可见，在工控系统中，攻防双方可能把主要精力放在了工控系统的控制设备、工业控制管理软件系统上。而且随着时间的推移，越来越多人开始关注PLC的安全问题。

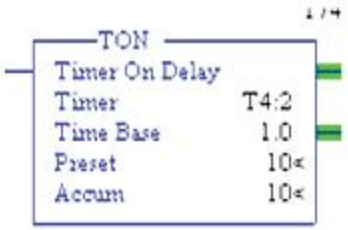
三、PLC安全研究

- PLC是专为工业控制而开发的装置，其主要使用者是工厂广大电气技术人员，为了适应他们的传统习惯和掌握能力，通常PLC不采用微机的编程语言，而常常采用面向控制过程、面向问题的“自然语言”编程。

- 国际电工委员会（IEC）1994年5月公布的IEC-61131-3（可编程控制器语言标准）规定了句法、语义和5种编程语言：功能表图（sequential function chart）、梯形图（Ladder diagram）、功能块图（Function black diagram）、指令表（Instruction list）、结构文本（structured text）。梯形图和功能块图为图形语言，指令表和结构文本为文字语言，功能表图是一种结构块控制流程图。

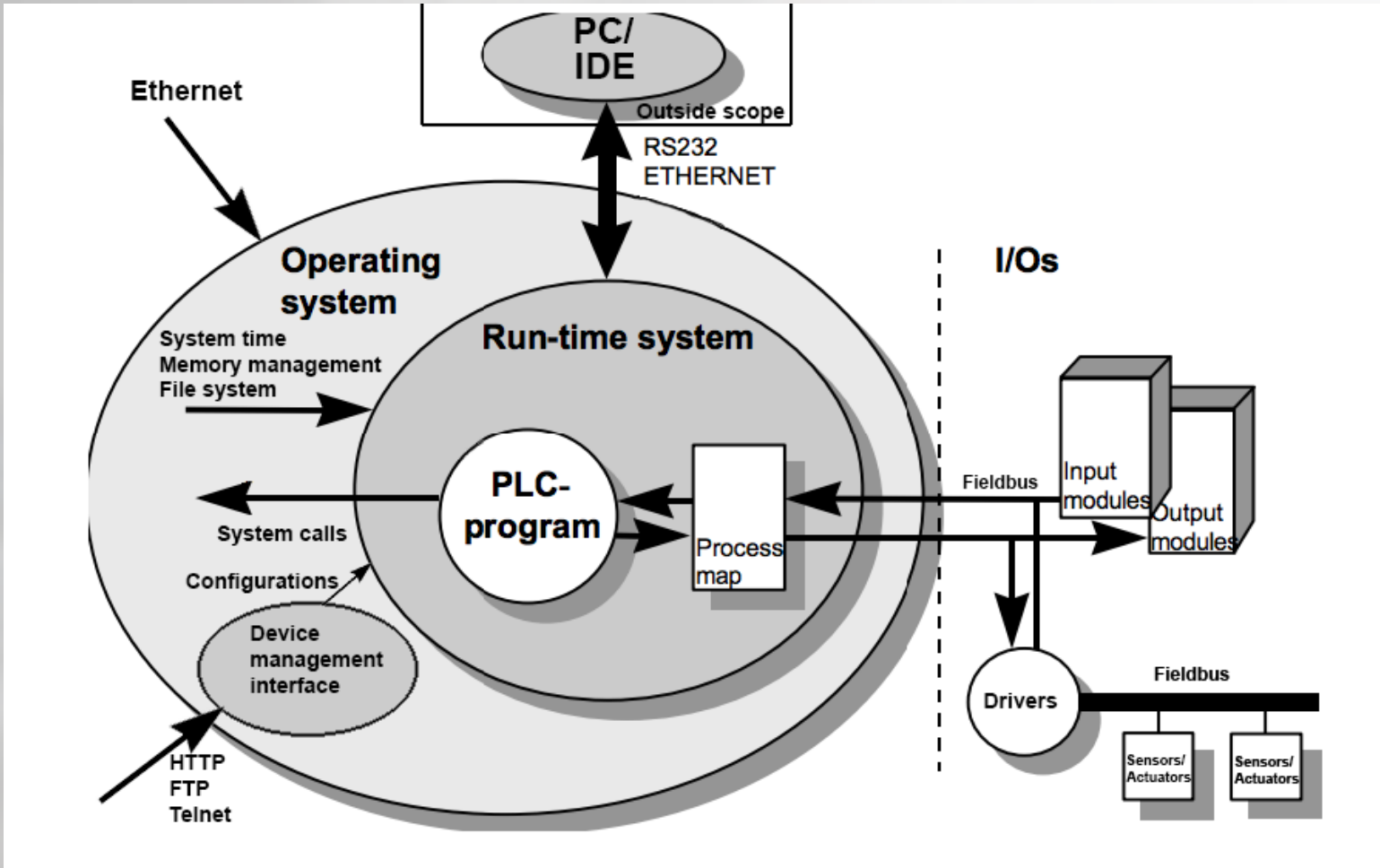

MITSUBISHI
RUN
MON
PRM
PU
EXT
NET
STOP RESET
RUN
MODE
SET
PU EXT
TAKE AWAY
CONVEYOR#1
E700
DANGER
CAUTION
DANGER
AVERTISSEMENT





Test for set conditions

Poll for input/generate output



从安全分析角度看，防范PLC的攻击面存在于：上位机PC、以太网的其它连接，提供的HTTP、FTP等服务接口，传感层（或者说现场层）的I/O输入等。

攻击者的目标和意图

PLC运行时系统

- 读工程文件
- 运行/终止梯形逻辑
- 上传梯形逻辑
- 下载梯形逻辑
- 查看梯形逻辑源码
- 改变梯形逻辑代码
- 读写总线
- 读写进程值
- 执行梯形逻辑

文件系统

- 读写文件
- 读写PLC配置文件
- 读写PLC运行时系统文件
- 删除文件
- 格式化文件系统
- 改变文件权限

控制器管理系统

- 重启PLC
- 恢复缺省设置
- 停止PLC
- 配置I/O模块

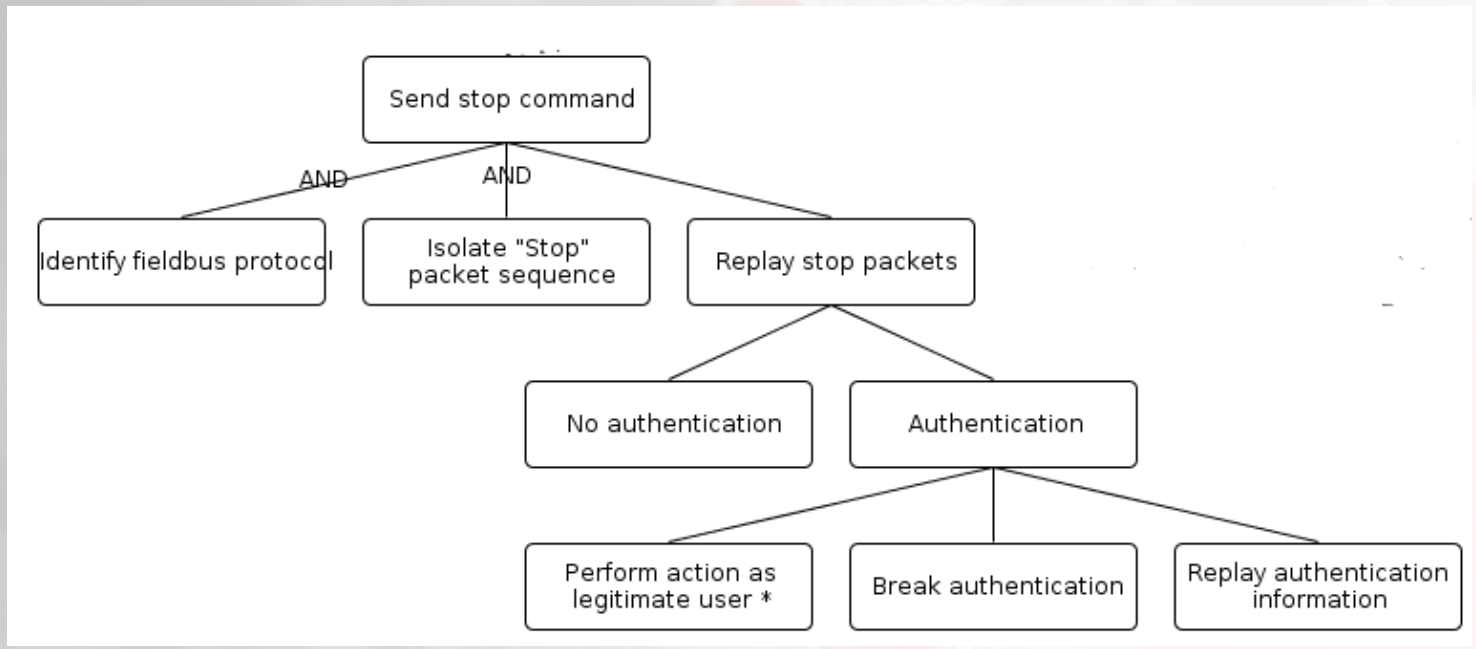
操作系统

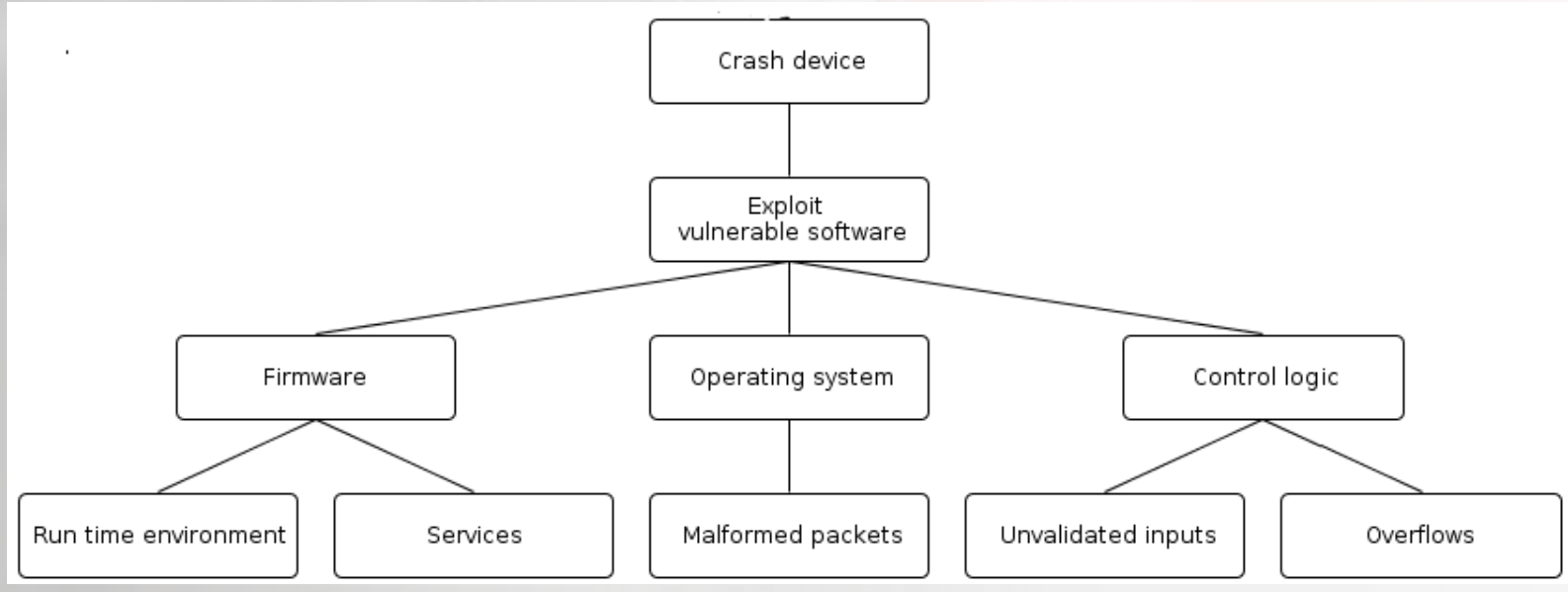
- 系统调用
- 通信
- 代码执行

固件

- 上传固件
- 下载固件
- 改变固件

“攻击树”模型


Send stop command
AND
AND
Identify fieldbus protocol
Isolate "Stop" packet sequence
Replay stop packets
No authentication
Authentication
Perform action as legitimate user *
Break authentication
Replay authentication information


Crash device
Exploit vulnerable software
Firmware
Operating system
Control logic
Run time environment
Services
Malformed packets
Unvalidated inputs
Overflows

PLC安全的概述

- J. Mulder, M. Schwartz, M. Berg, J. V. Houten, J. Urrea, and A. Pease, “Analysis of Field Devices Used in Industrial Control Systems,” in Critical Infrastructure Protection VI. Springer, 2012, pp. 45 -57，分析了PLC的弱点，包括硬件、固件、背板通信分析。
- L. McMinn, “External Verification of SCADA System Embedded Controller
- Firmware,” Master’s thesis, Air Force Institute of Technology, March 2012.，外部验证工具用于记录和监视PLC的所有更新，本质上提供了基于硬件的配置管理。
- C. Bellettini and J. Rrushi, “Combating Memory Corruption Attacks on SCADA Devices,” Critical Infrastructure Protection II, vol. 290, pp. 141 -156, 2009，提出了加密内存的保护方式，来防止恶意代码修改。
- K. Sickendick, “File Carving and Malware Identification Algorithms Applied to Firmware Reverse Engineering,” Master’s thesis, Air Force Institute of Technology,March 2013

- S. Dunlap, “Timing-Based Side Channel Analysis in the Industrial Control System Environment,” Master’s thesis, Air Force Institute of Technology, June 2013.使用PLC执行时间作为边信道来检测潜在的威胁的PLC，PLC与工作站不同，其行为固定，固定时间的约束提供了非授权修改检测的有效尺度。
- Z. Basnight, J. Butts, J. L. Jr, and T. Dube, “Firmware Modification Attacks on Programmable Logic Controllers,” International Journal of Critical Infrastructure Protection, 2013,由于嵌入式设备缺乏较强的认证、输入的验证、文件完整性验证等，可能会导致固件被篡改。
- 值得注意的是：单个PLC可能是多个不同厂商例如ARM和PPC等不同类型处理器的混合。S7-200包含德州仪器处理器、AMD驱动的flash memory，Atmel的模拟I/O的芯片等。

Firmware的问题

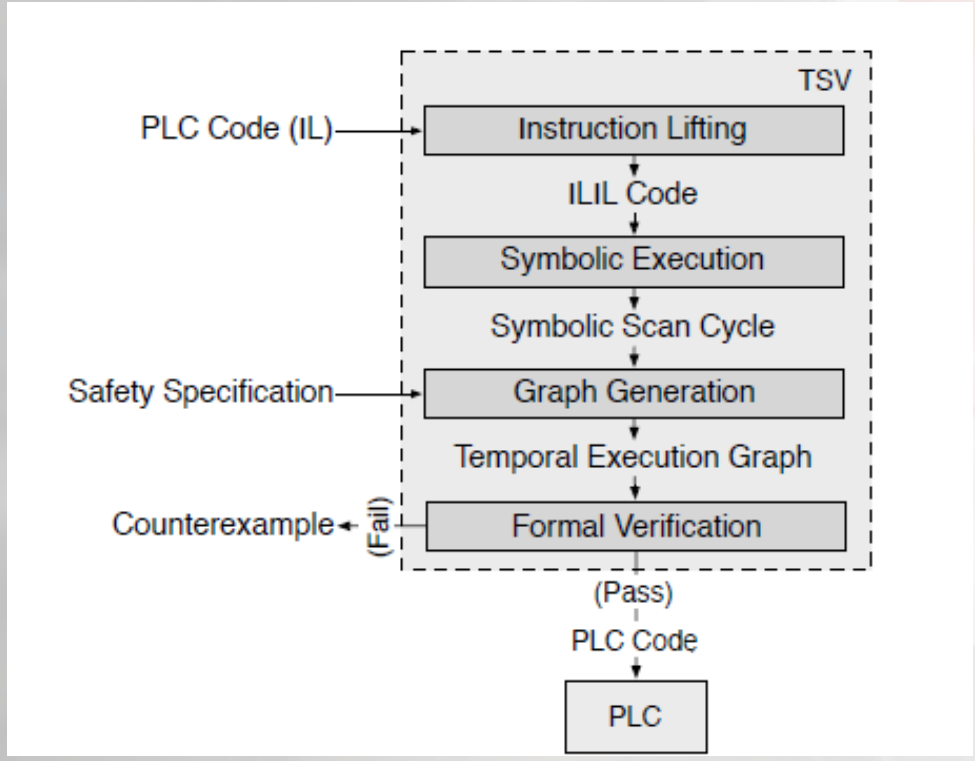
- 罗克韦尔 1756 ENBT Ethernet module 和 光洋 (KOYO) H4-ECOM100 Ethernet module

By disassembling the binary firmware, they were able to fingerprint the system and reverse engineer the format of the firmware and the checksum algorithm.

1756 ENBT Modules

H4-ECOM100

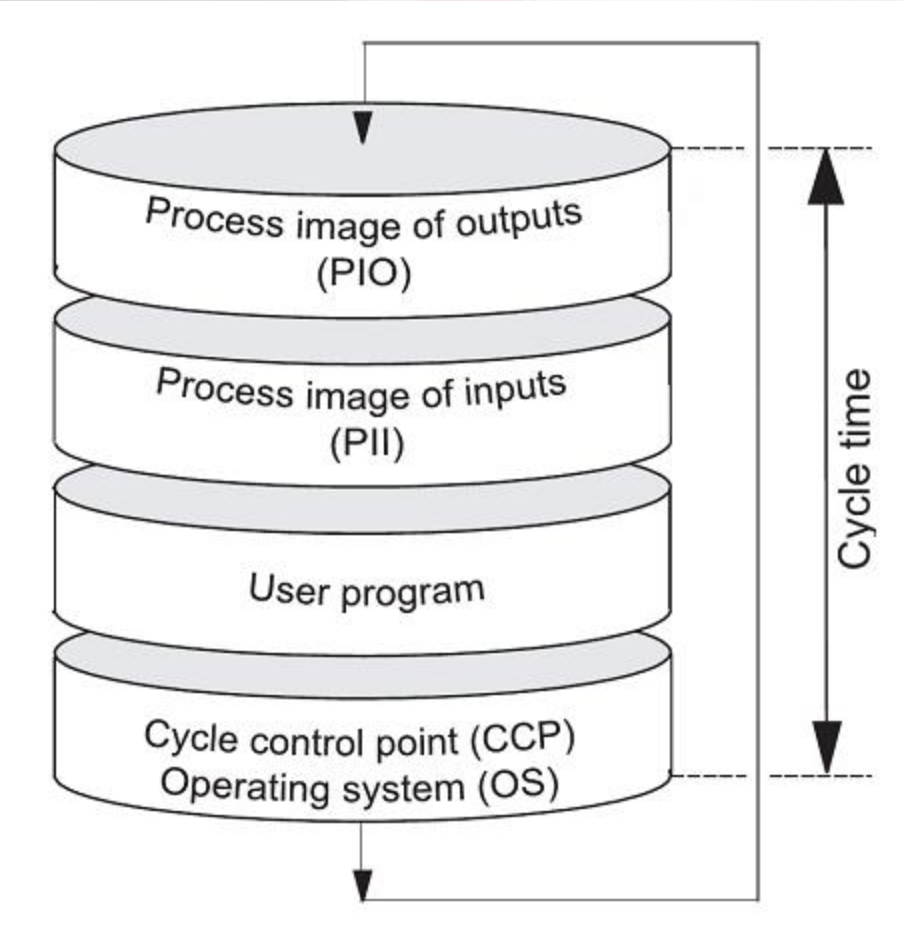
A Trusted Safety Verifier for Process Controller Code—TSV架构



引入了符号执行的方法：

a minimal TCB for the verification of safety-critical code executed on programmable controllers. No controller code is allowed to be executed before it passes physical safety checks by TSV.

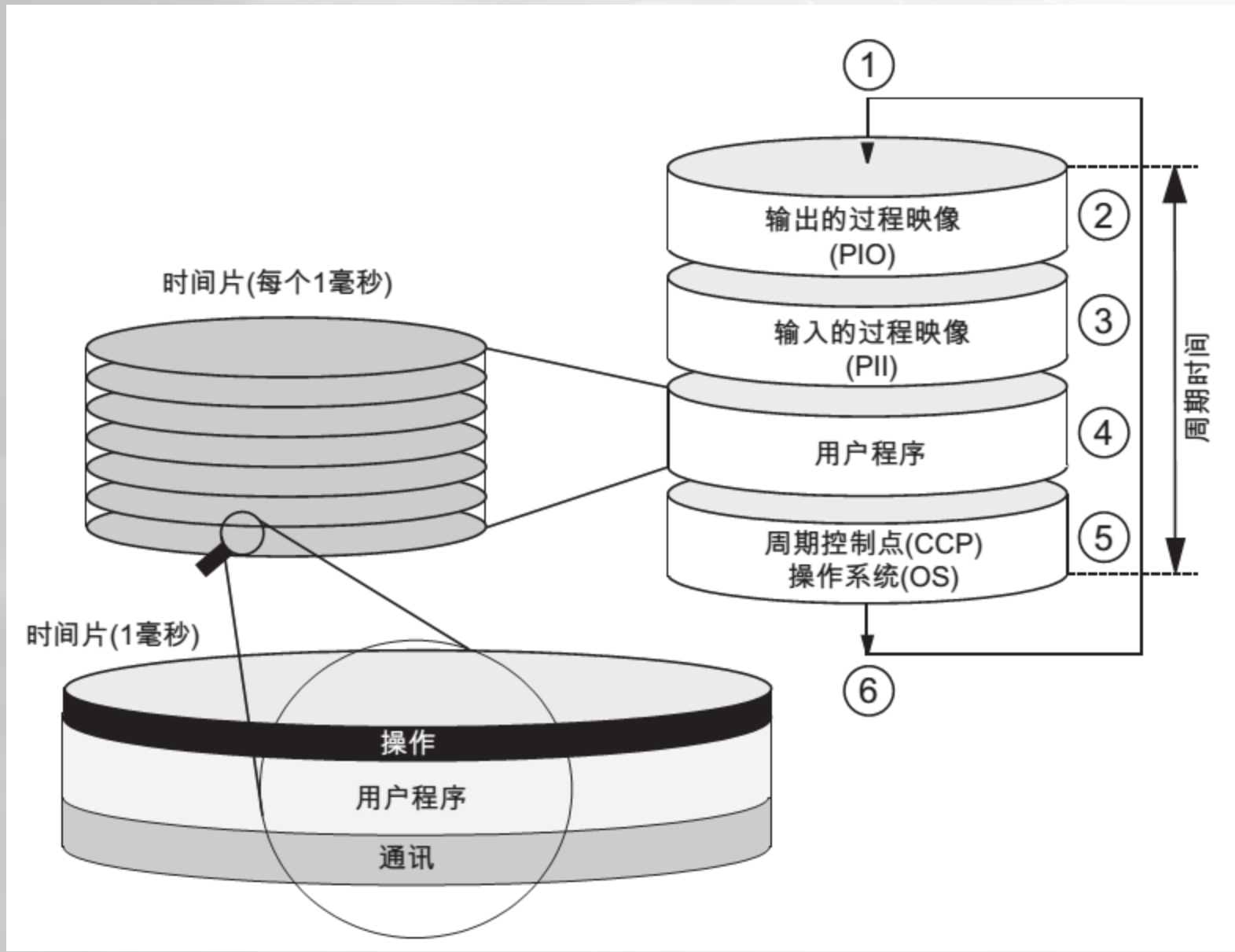
西门子PLC相关



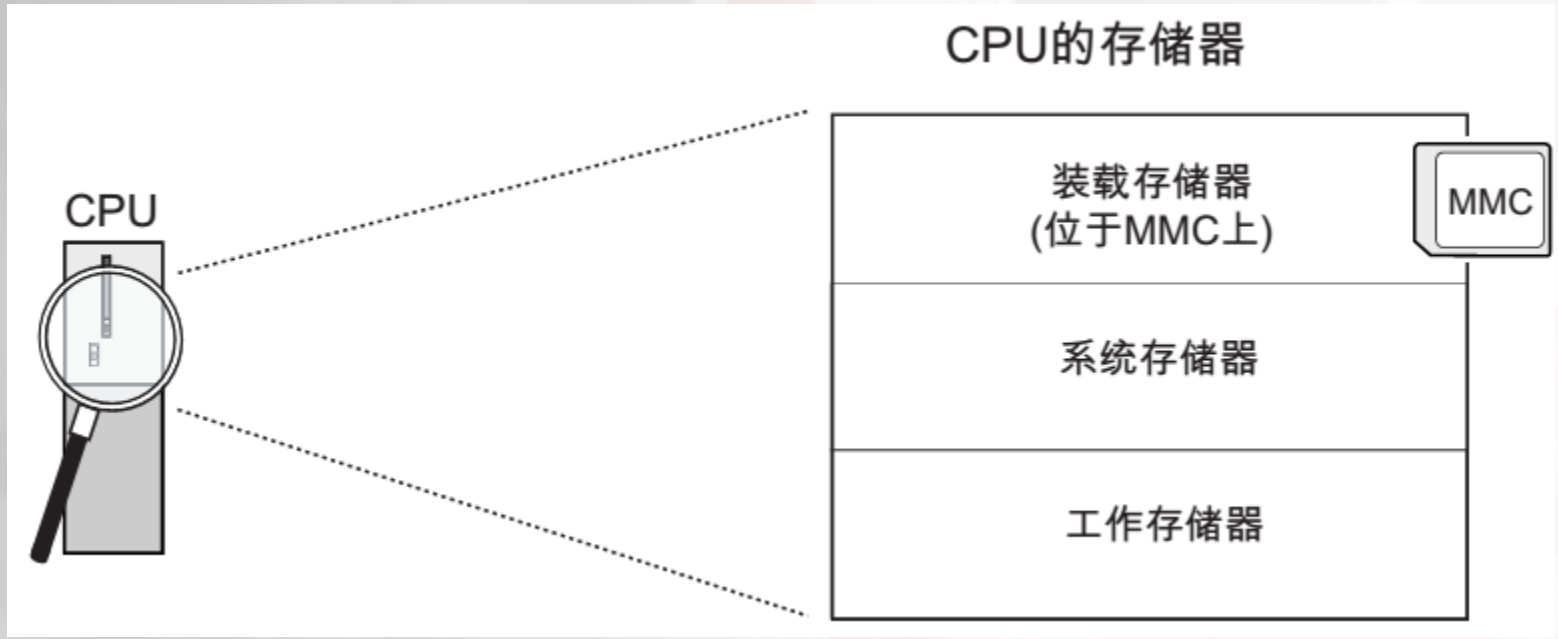
- 循环执行模型及I/O

程序结构和组织

Block type		Description
Organization Block	OB	Program entry point
Data Block	DB	Data storage
Function	FC	Function
Function Blocks	FB	Stateful function
System Functions	SFC, SFB	System library
System Data Blocks	SDB	PLC configuration



SIEMENS S7-300、CPU31XC和CPU31X的技术数据手册



装载存储器位于 SIMATIC 微存储卡 (MMC) 上。装载存储器与 SIMATIC 微存储卡的大小完全相同。它用来存储代码块、数据块和系统数据（组态、连接、模块参数等）。标识为与运行时间无关的块被专门存储在装载存储器中。也可在 SIMATIC 微存储卡上存储项目的所有组态数据。

注意

只有在 CPU 中插入 SIMATIC 微存储卡后，才能下载用户程序，因此才能使用 CPU。

Boolean term:

- `Q0.0 = (I0.0 ∧ I0.1) ∨ I0.2`

Statement List (STL):

```
A    %I0.0
A    %I0.1
O    %I0.2
=    %Q0.0
```

OB 1 with

```
A %I0.0
A %I0.1
O %I0.2
= %Q0.0
```

is compiled to

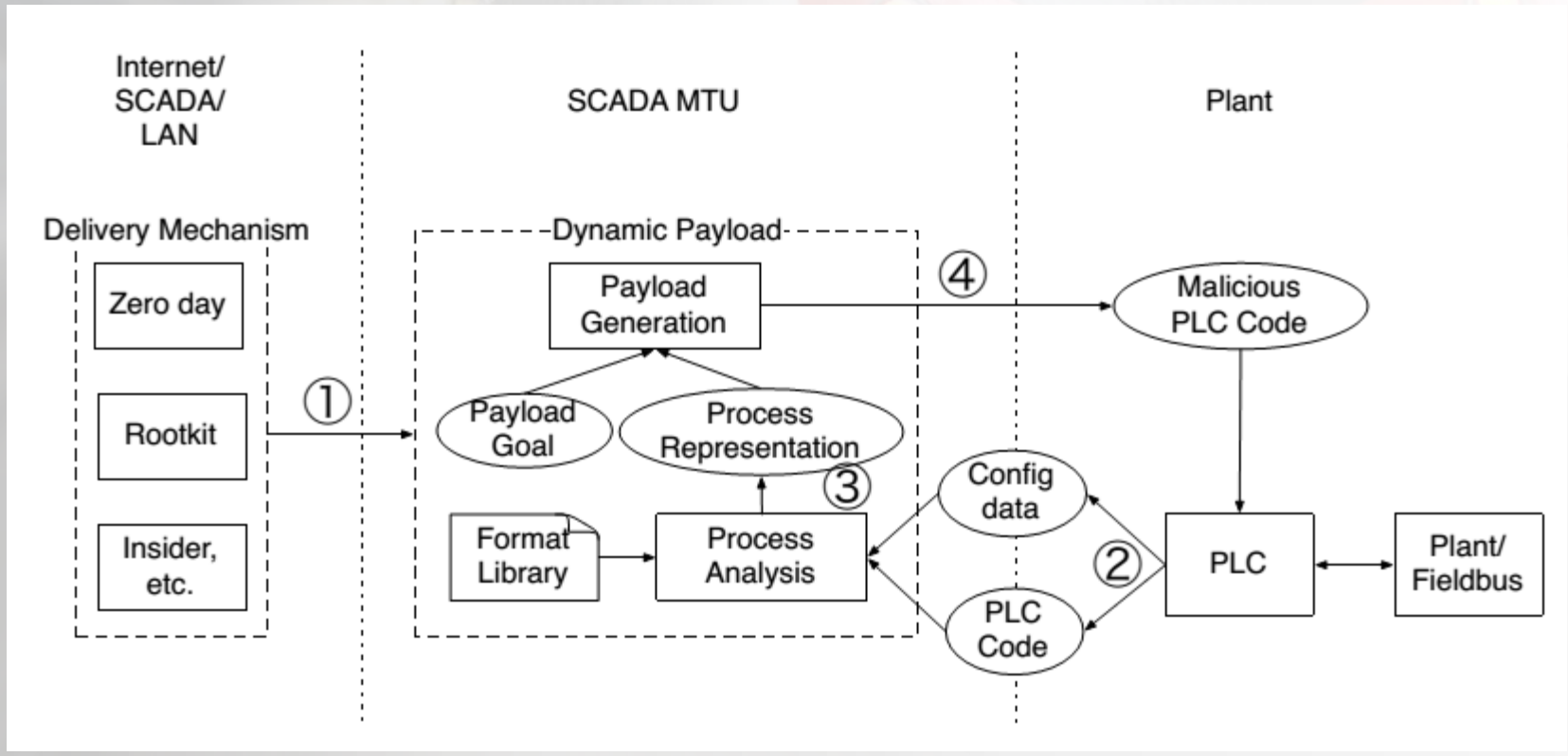
```
00: 7070 0101 0108 0001 0000 0074 0000 0000
10: 02ab 2735 2d03 03a1 6383 21a7 001c 0006
20: 0014 000a c000 c100 ca00 d880 6500 0100
30: 0014 0000 0002 0502 0502 0502 0502 0502
40: 0505 0505 0505 050e 0520 0100 0800 0000
50: 0000 0000 0000 0000 0000 0000 0000 0000
60: 0000 0000 0000 0000 0100 a691 0000 0000
70: 0000 0000
```

PLC代码的逻辑验证问题

- 一个PLC程序可以看作一个逻辑，每秒有多次的循环执行，每次执行可以称作一个扫描周期；
- 在每次扫描周期，有从工厂的各个传感器输入标量I，逻辑处理产生的一组输出变量O，传递给物理设备的动作行为，逻辑还维护一组内部状态变量C，以及时钟变量T。以西门子的S7为例，就为I，O，C，T分别提供了独立的内存区域。
- 不论PLC上的程序以何种形式语言编程，大多数PLC程序都可以看作是一组布尔表达式φ.因此，可以采用基于IR的逻辑验证方法。
- N. G. Ferreira. Automatic Verification of Safety Rules for a Subway Control Software. In Proceedings of the Brazilian Symposium on Formal Methods(SBMF), 2004.
- T. Park and P. I. Barton. Formal Verification of Sequence Controllers. Computers & Chemical Engineering.
- G.Canet,Towards The automatic verification of PLC program written in Instruction List.In Proc. IEEE Conf. Systems, Man and Cybernetics(SMC 2000) pages 2449-2454.

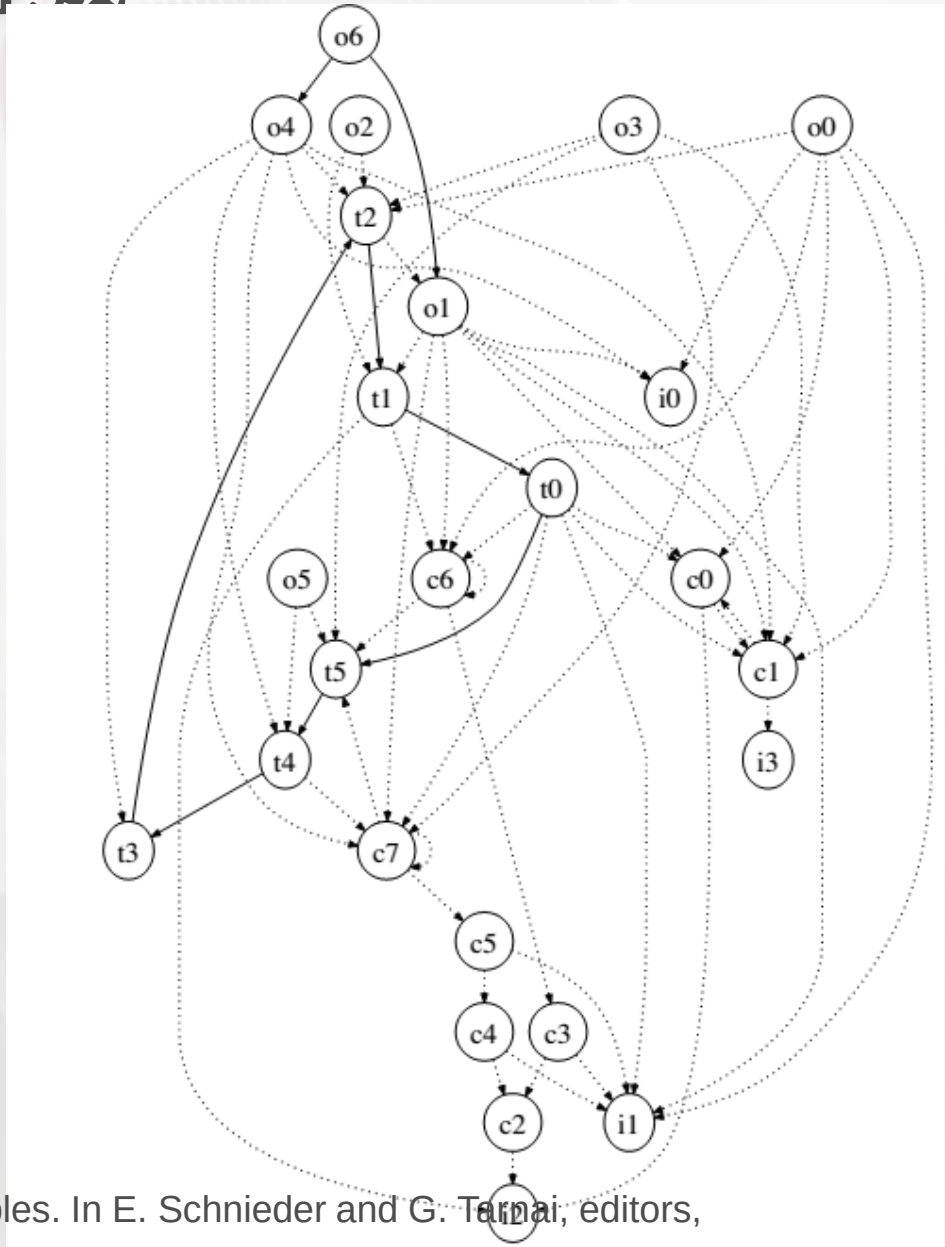
PLC恶意代码载荷的生成

- 来自南加州大学的S.McLaughlin最早研究
- “On dynamic malware payloads aimed at programmable logic controllers.” in HotSec, 2011.
- payload的产生包括：推断safety interlock，导致系统进入非安全状态



PLC恶意代码载荷的生成

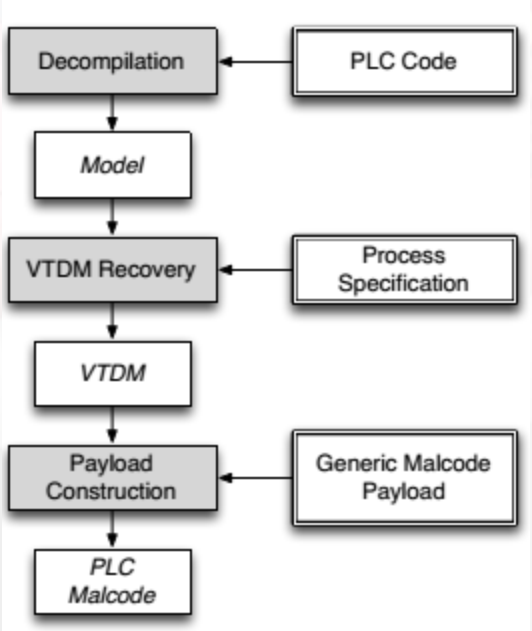
- 推断工厂结构和目的
- 以交通信号控制为例
- 6个定时器组成的循环，
- 输出变量o6依赖于o1, o4
- 作为终止条件，o6互锁于o1、o4，当两个相反的绿灯o1，o4同时激活，o6触发报警。
- 因此，赋值o1<-1, o4<-1, o6<-0，就是非安全状态。构造之！



A. Ferrari, Model Checking Interlocking Control Tables. In E. Schnieder and G. Tarnai, editors, FORMS/FORMAT 2010. 2011.

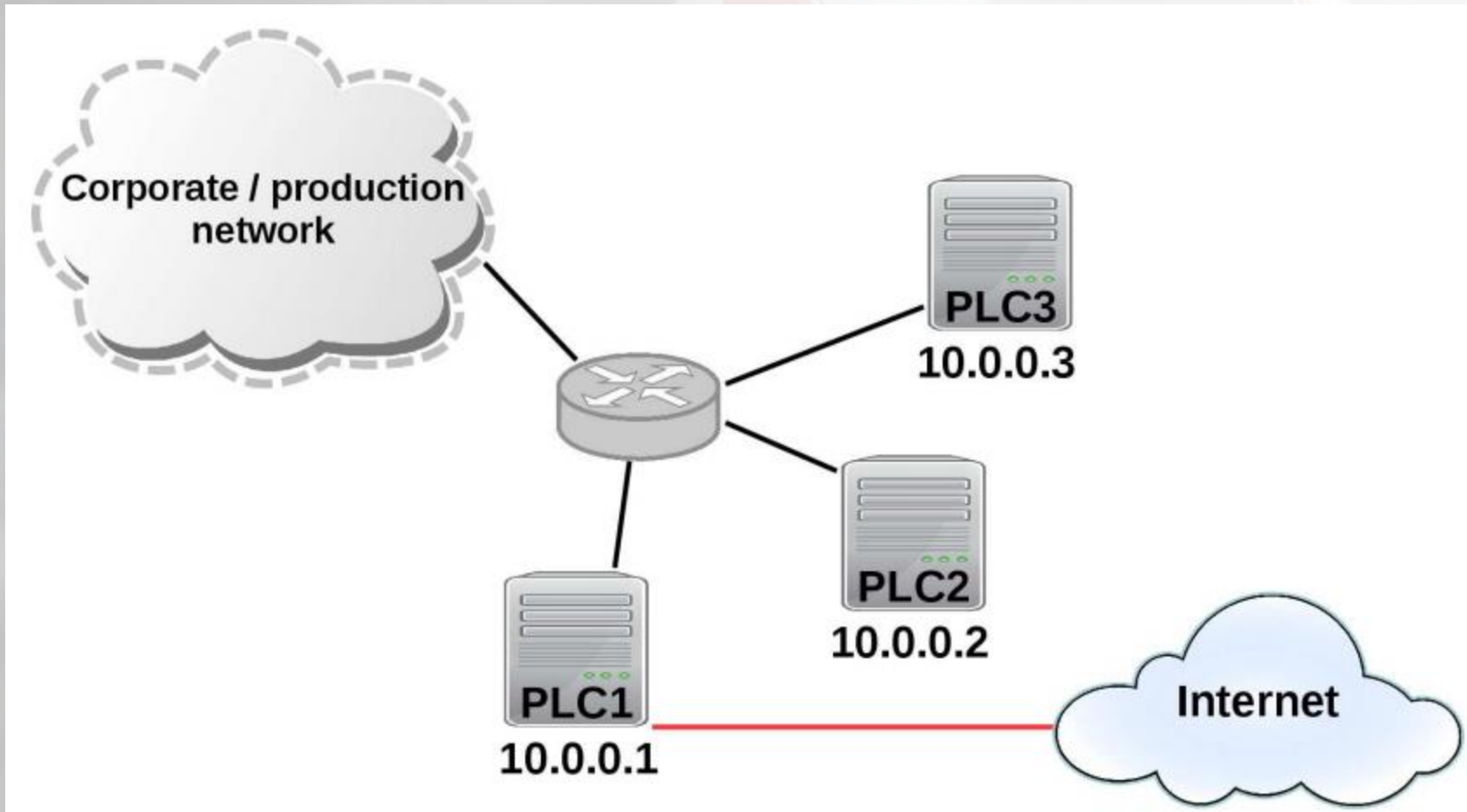
SABOT：基于规则的PLC攻击载荷生成

- CCS 2012
- 核心目标：恢复PLC内存位置的语义，并且与物理设备相匹配
- Variable To Device Mapping
- Decompilation：将控制逻辑的字节
- 码形式翻译成约束的中间表示形式，
- 再将该约束翻译成NuSMV模型检测
- 工具接受的语言M。

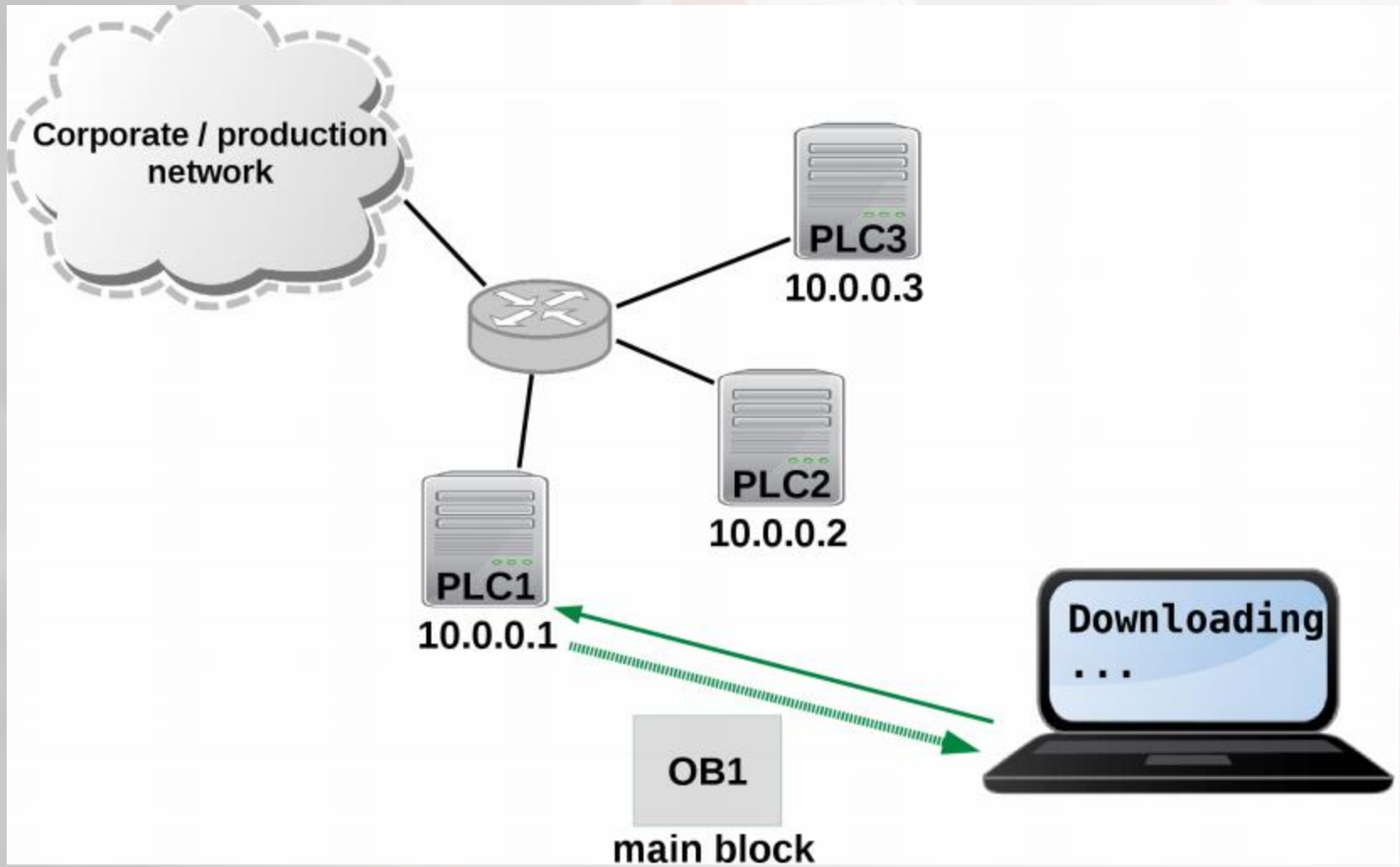


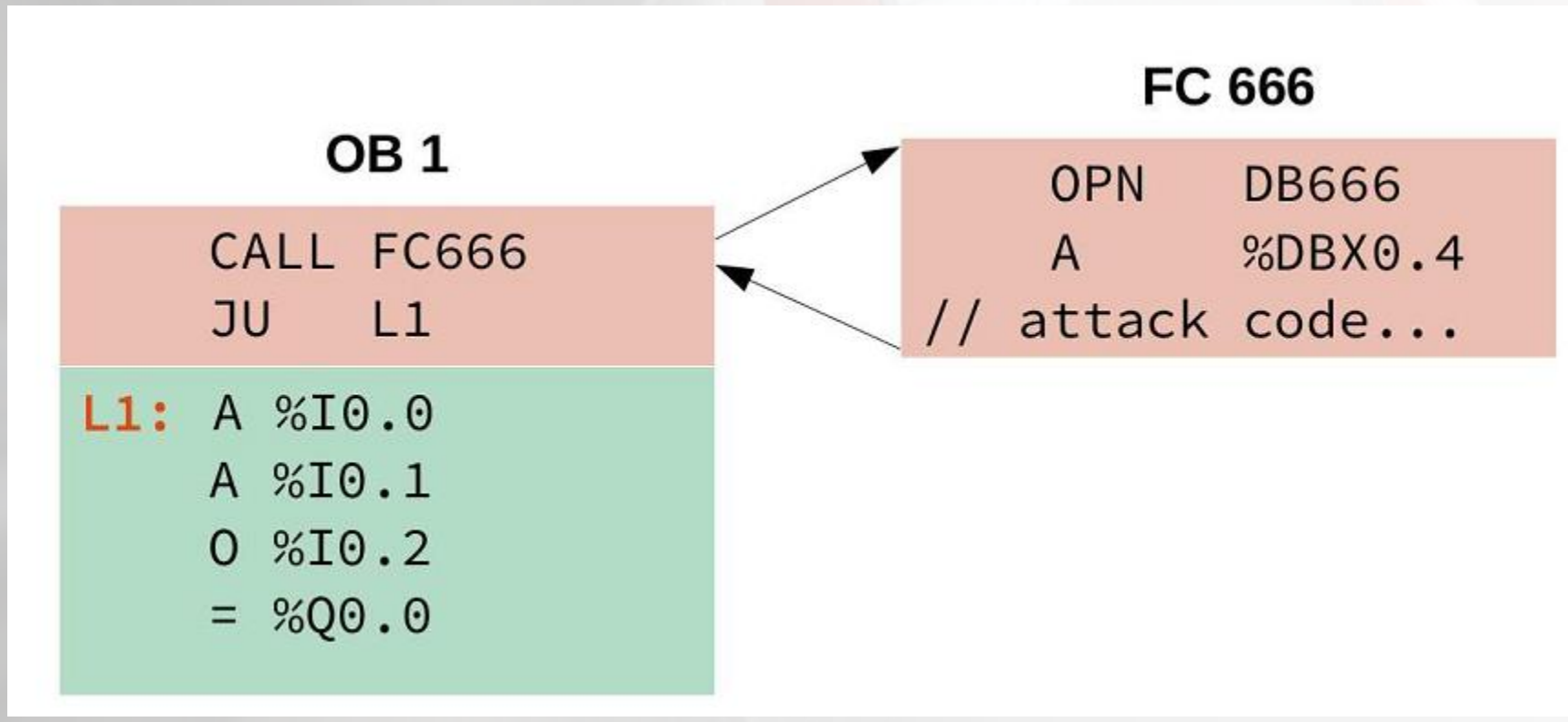
Internet-Facing PLCs - A New Back Orifice

- Johannes Klick, BlackHat 2015
- Introduction
  - Traditional Attack Vectors
  - Internet-facing PLCs
  - Generell Attack Overview
- Siemens PLCs
  - STL Language and its MC7 Bytecode
  - S7Comm Protocol (downloading program b
- Attack Details
  - PLC Code Injection with PLCinject (Demo
  - SNMP Scanner & SOCKS Proxy in STL



PLC 1 is connected to the Internet

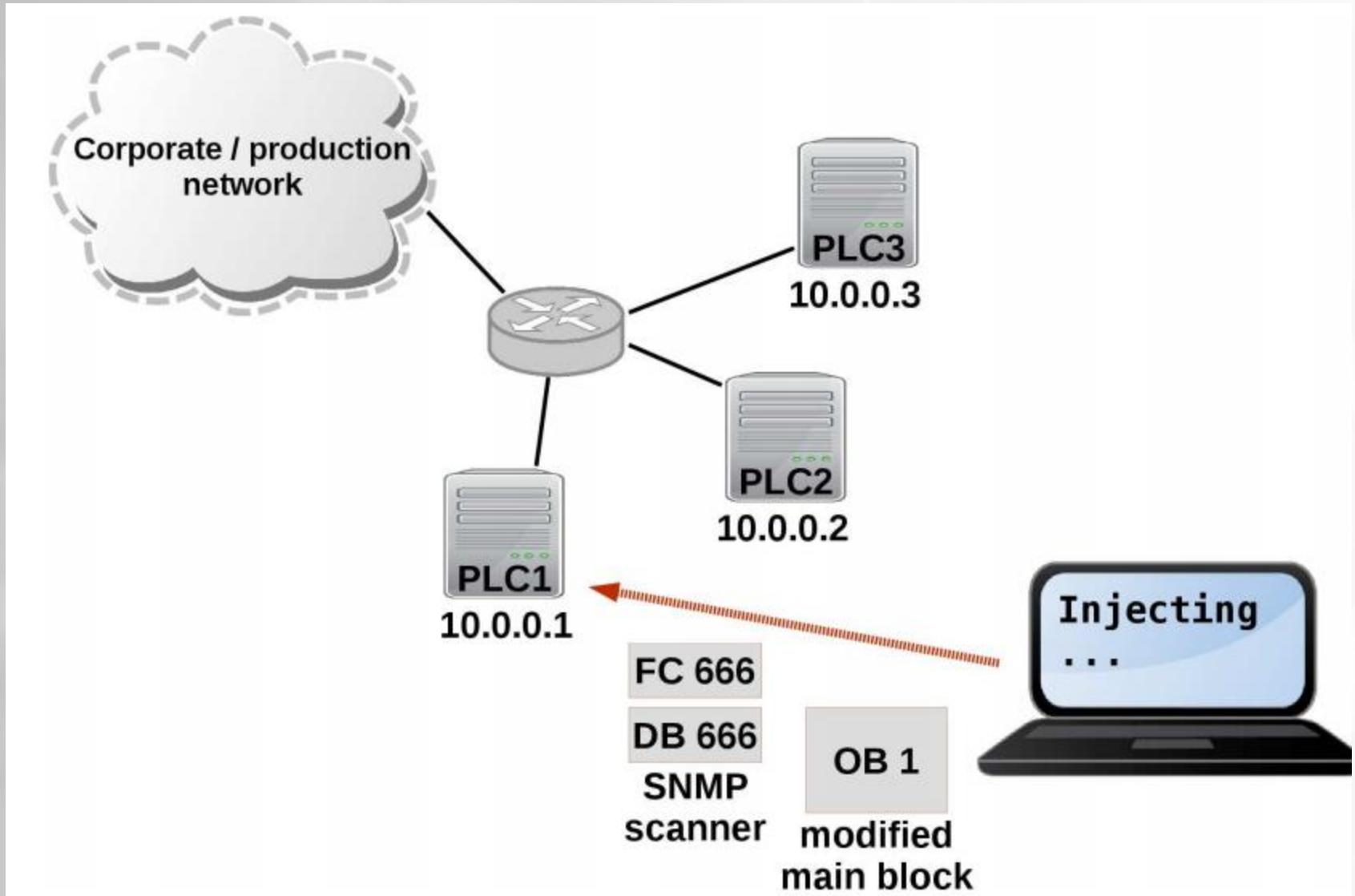

Corporate / production network
PLC3
10.0.0.3
PLC2
10.0.0.2
PLC1
10.0.0.1
Downloading
...
OB1
main block


OB 1
CALL FC666
JU L1
L1: A %I0.0
A %I0.1
O %I0.2
= %Q0.0
FC 666
OPN DB666
A %DBX0.4
// attack code...

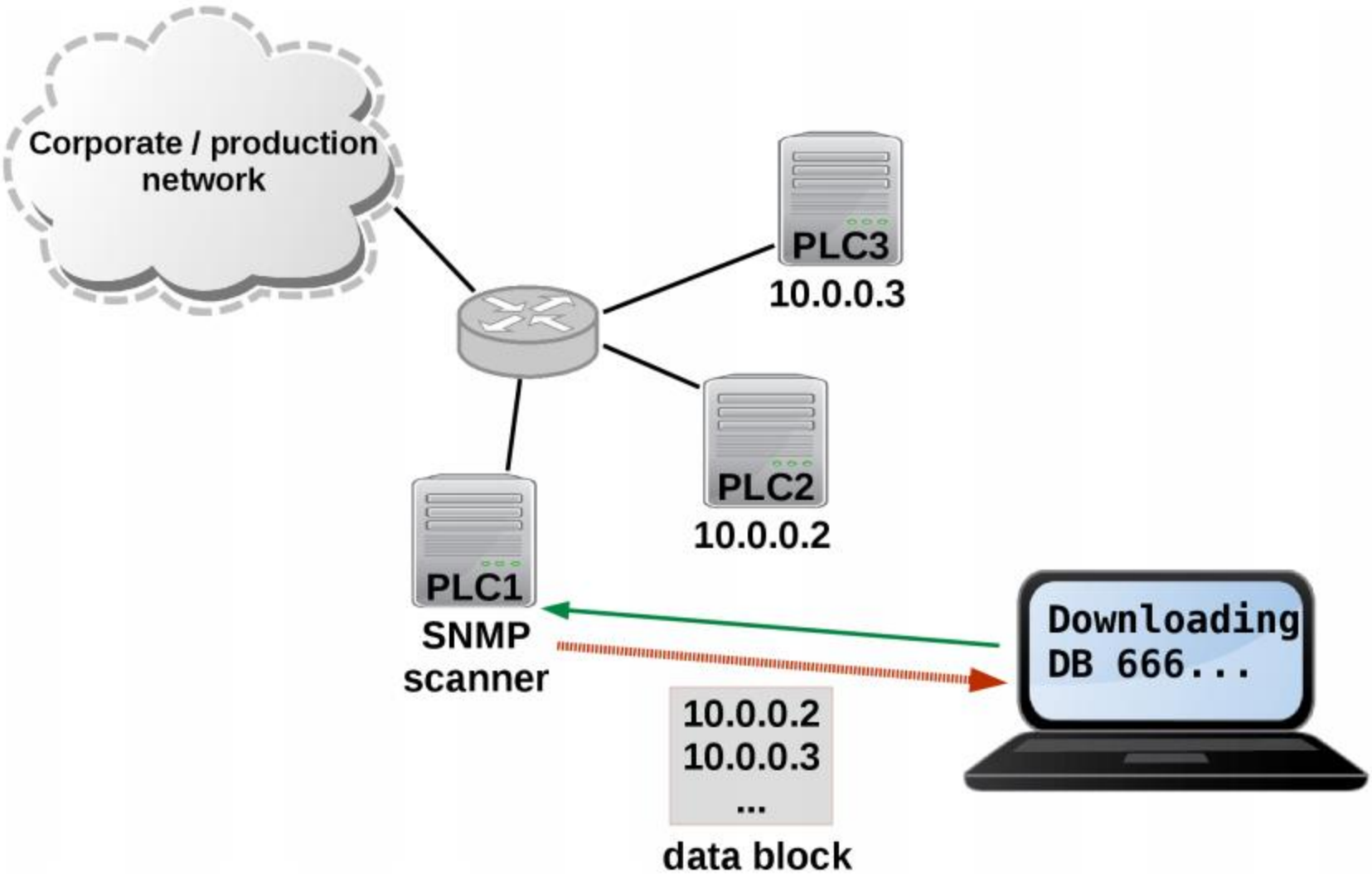
```
     CALL FC666
     JU L1
L1:  A %I0.0
     A %I0.1
     O %I0.2
     = %Q0.0
     BE
```

1. insert block call
2. increase total block length
3. increase code length

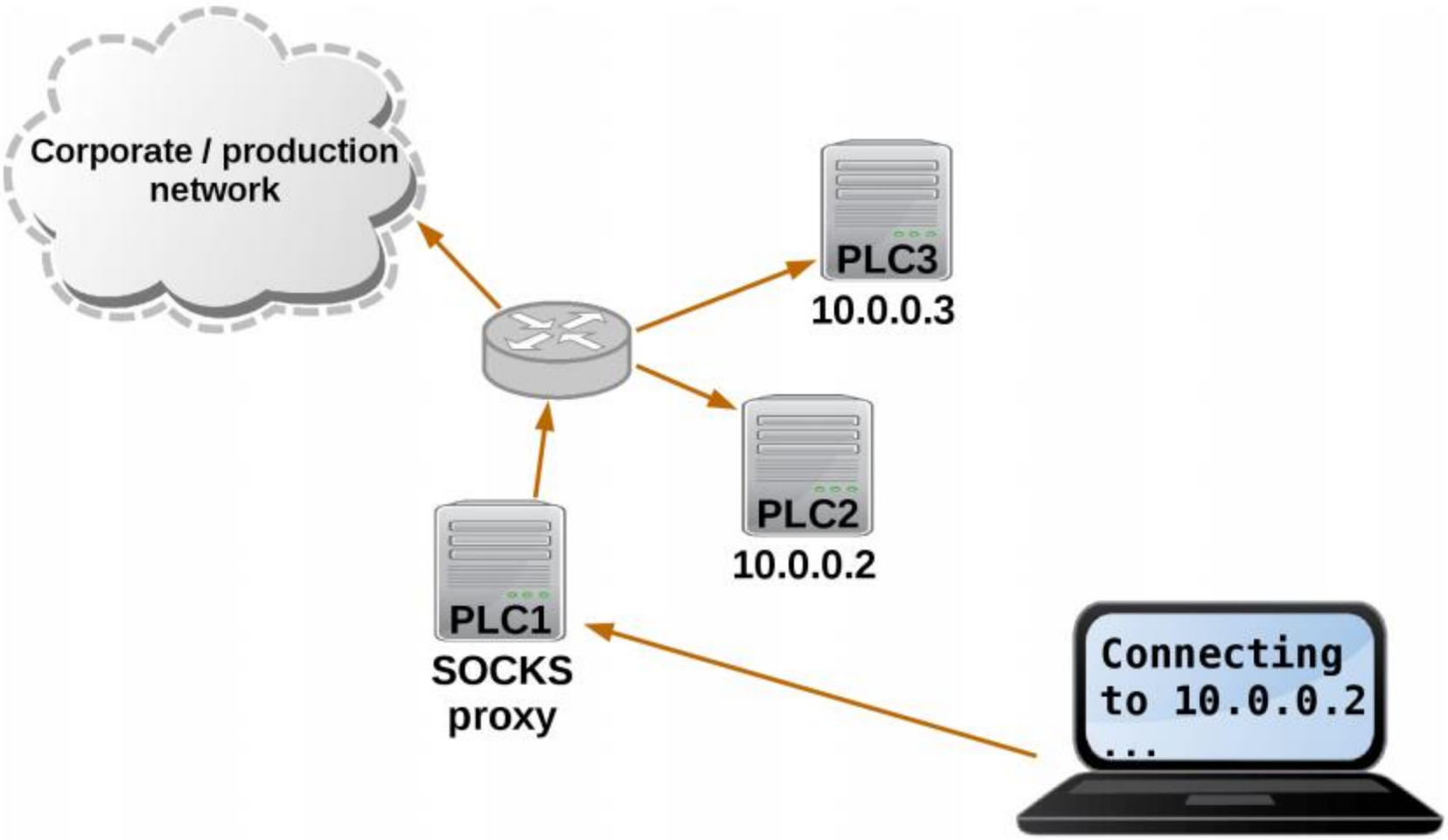
```
00:  7070 0101 0108 0001 0000 007C 0000 0000
10:  02ab 2735 2d03 03a1 6383 21a7 001c 0006
20:  0014 0012 fb70 029a 700b 0002 c000 c100
30:  ca00 d880 6500 0100 0014 0000 0002 0502
40:  0502 0502 0502 0502 0505 0505 0505 ...
```



. . . patches it and uploads a SNMP scanner



Attacker downloads the scanning results

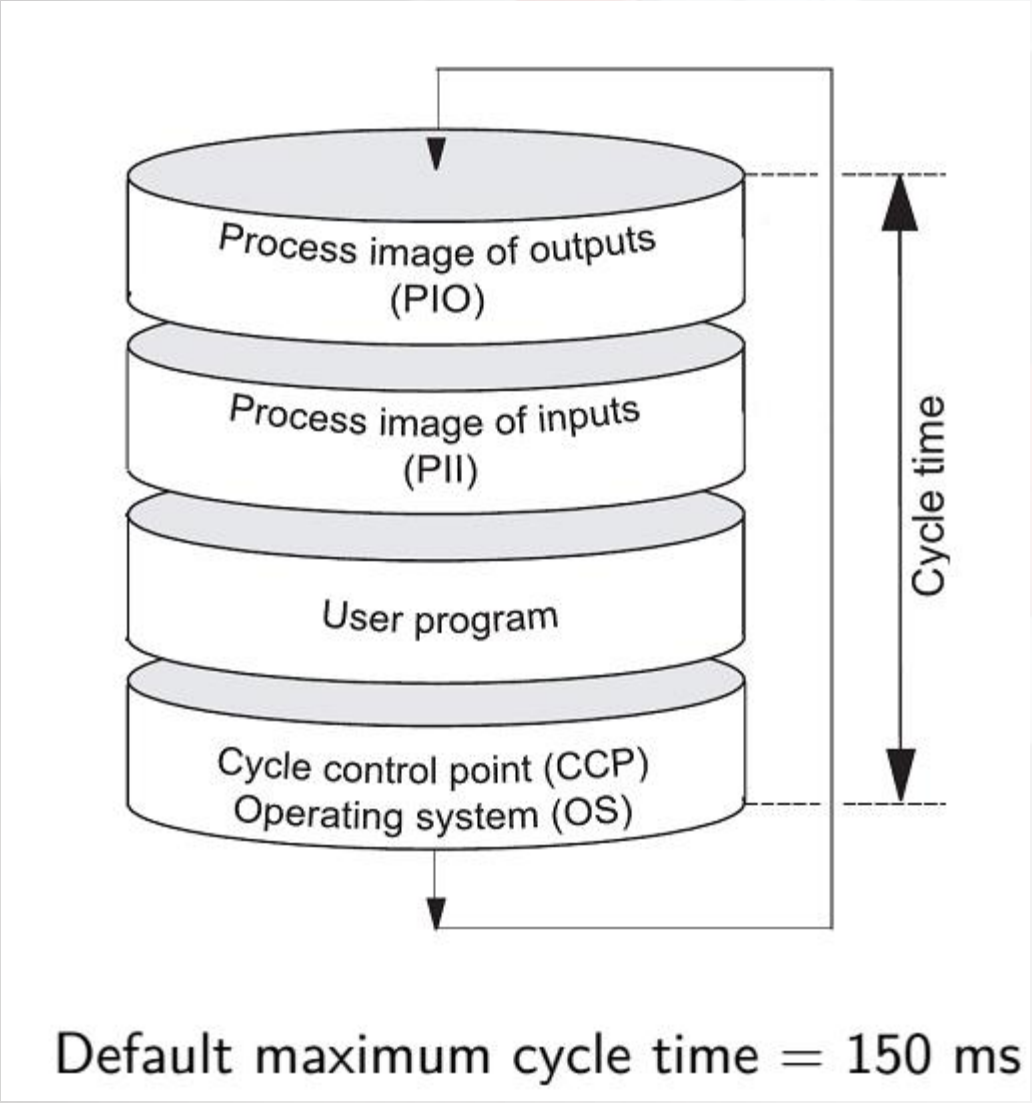


A SOCKS proxy enables him to reach the net behind the PLC

```
0001 get_ip : NOP 1
0002
0003 // read ip from system state list (SZL)
0004       CALL  RDSYSST
0005          REQ         :=TRUE
0006          SZL_ID      :=W#16#0037
0007          INDEX       :=W#16#0000
0008          RET_VAL     :=#sysst_ret
0009          BUSY        :=#sysst_busy
0010          SZL_HEADER  :="DB".szlheader.SZL_HEADER
0011          DR          :="DB".ip_info
0012
0013 // wait until SZL read finished
0014       A     #sysst_busy
0015       BEC
0016
0017       SET
0018       S     #got_ip
```

Get the PLC's IP

注意的问题


Process image of outputs
(PIO)
Process image of inputs
(PII)
User program
Cycle control point (CCP)
Operating system (OS)
Cycle time
Default maximum cycle time = 150 ms

四、现实与展望

工业控制系统防护之难

1. **Safety要求高！**
   一旦做出危害性行为，后果不可估量
   安全性、鲁棒性、实时性要求高

2. **Update比较困难**
   宕机和重启可能是灾难性的

3. **有限的计算能力**
   产品成本、恶劣环境、简单可靠

现有防护方案

防护体系类：

•纵深防御

•Deep Defense

防护策略方案类：

①基于ICS、SCADA安全域的防护策略，安全分区、多层防护、横向隔离、纵向认证的电力系统防护方案，②异常检测、专用网络专用隔离、加密认证的scada安全防护方案，③区域隔离、通信管控、实时报警的多芬诺防护方案、

……

•防护技术类：

•网闸、防火墙、

•白名单、白环境、

•异常检测、IDS、IPS等

Seven Steps to Effectively Defend Industrial Control Systems

DHS/FBI/NSA. December 2015.

This paper presents seven strategies that can be implemented today to counter common exploitable weaknesses in “as-built” control systems. Length is 6 pages.

如何改变

“四不”出发点

不陷于“内存端”的攻防

与传统PC安全不同，
内存端20年战争。
工控有其安全特殊性

不排斥“兼容并”的增益

企图解决所有问题的观念本身就是错误的——杰奎斯法则

不拘泥“软件层”的局部

攻击在哪里发生？系统的谁更底层？

不改变“生态链”的继承

逐步兼容、逐步替代、非全部摒弃、重新设计。

小结

- 与IT安全的异同、发展轨迹值得关注，提升安全首先从改变观念做起；
- 攻击本身有可能需要结合信息流和能量流等，与一般IT安全有所不同；
- 针对PLC及其运行时环境的攻击越来越普遍，针对工控设备现场层设备的分析工具开始出现，比如ibal等。
- 控制层设备（围绕PLC相关）的安全更核心，漏洞分析等相关技术越来越向工控系统的底层深入。固件、操作系统、运行时系统越来越被“关注”。
- 从纵深防御到内生安全的整体发展，可适度加强动态防御及内生安全的组合使用

谢谢！ Q&A?