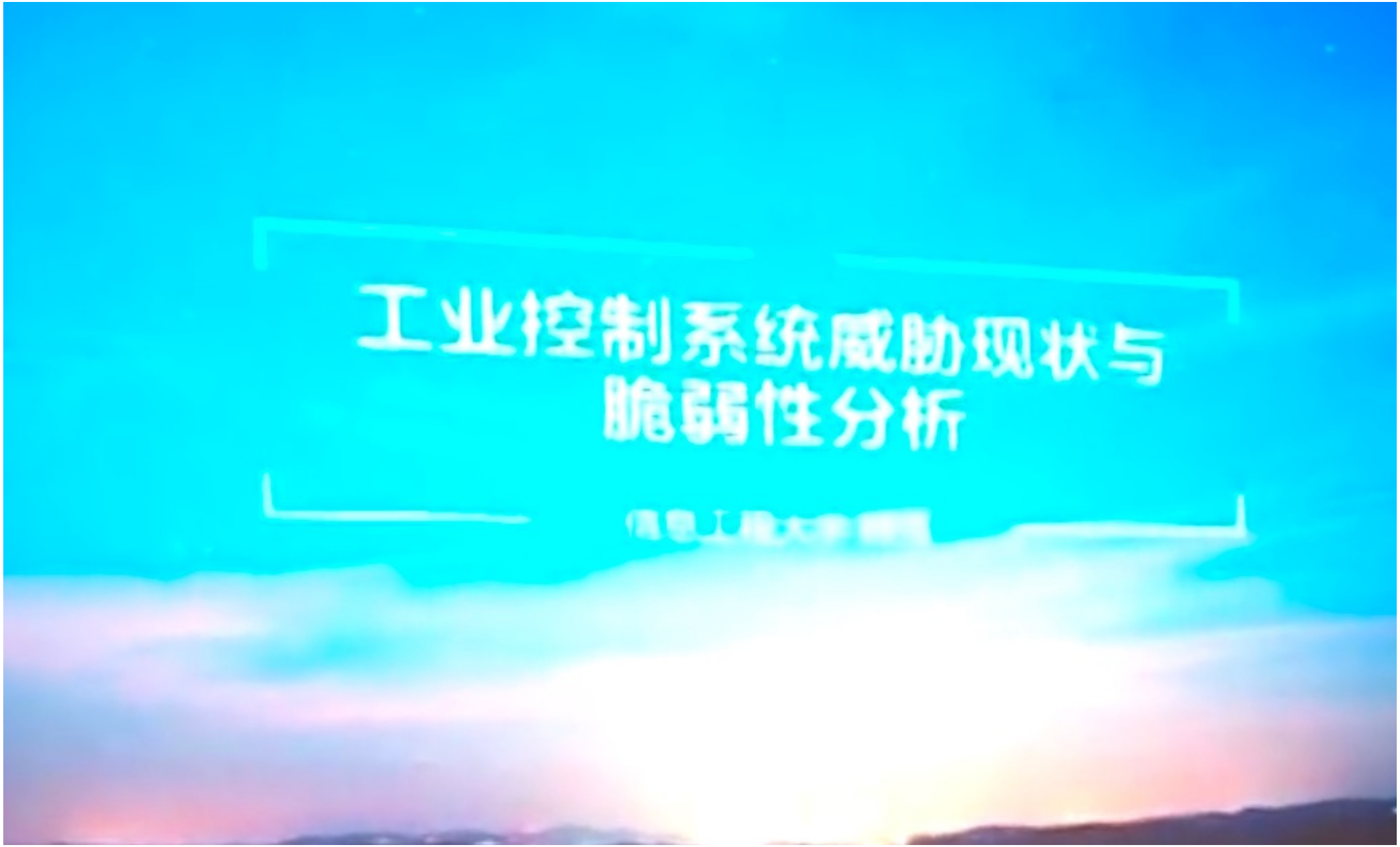


Hack Inn独家整理发布

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

三、重点聚焦：PLC安全研究

四、防护之难：现实与展望

Hack Inn独家整理发布

- 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[illegible]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。

腾讯视频

Hack Inn独家整理发布

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 / Ethernet 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 awareness"
D.6 "Access points to ICSs are easily controlled"
D.7 "Security is a problem that needs to be solved only once"

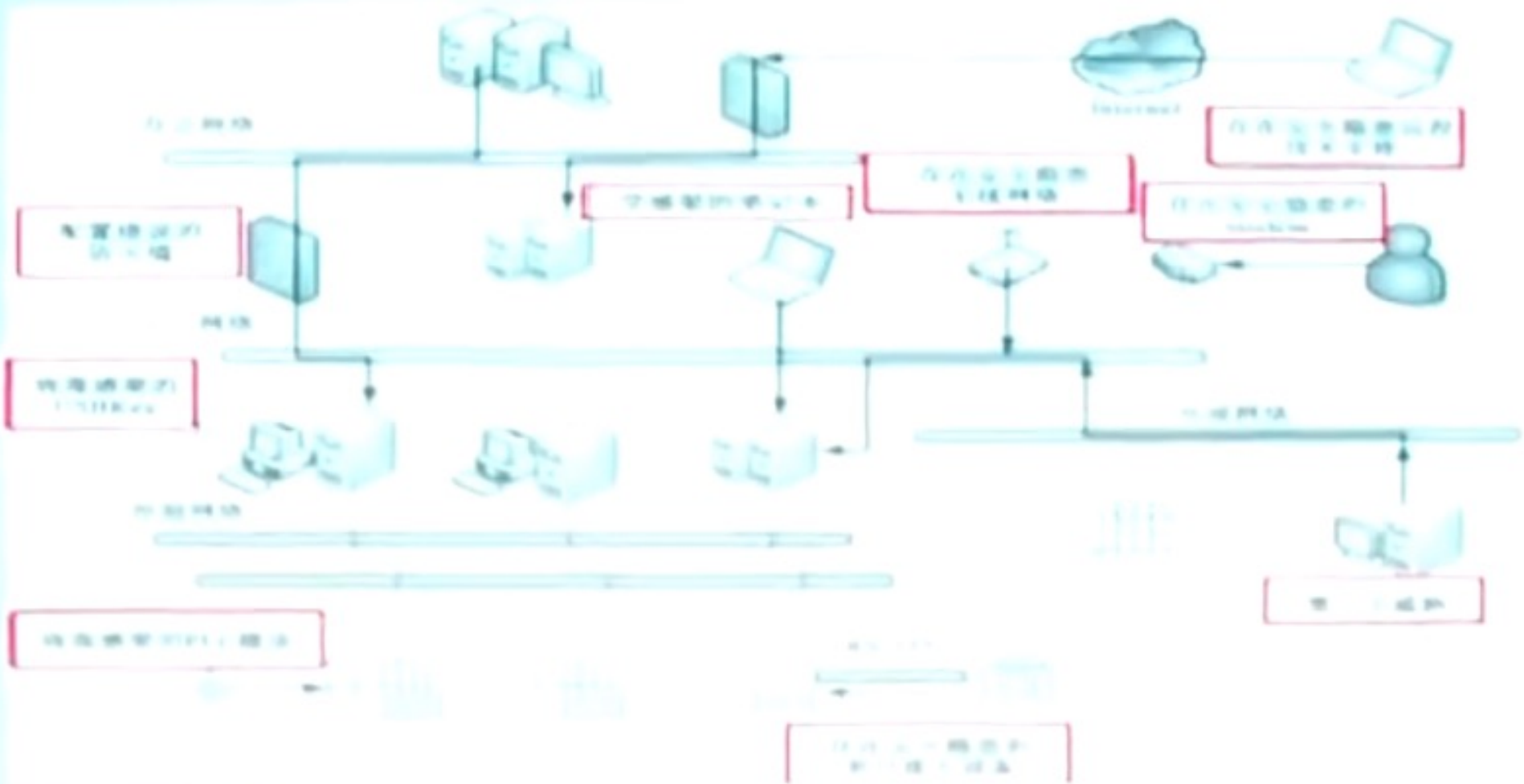
Hack Inn独家整理发布

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

Hack Inn独家整理发布

威胁建模



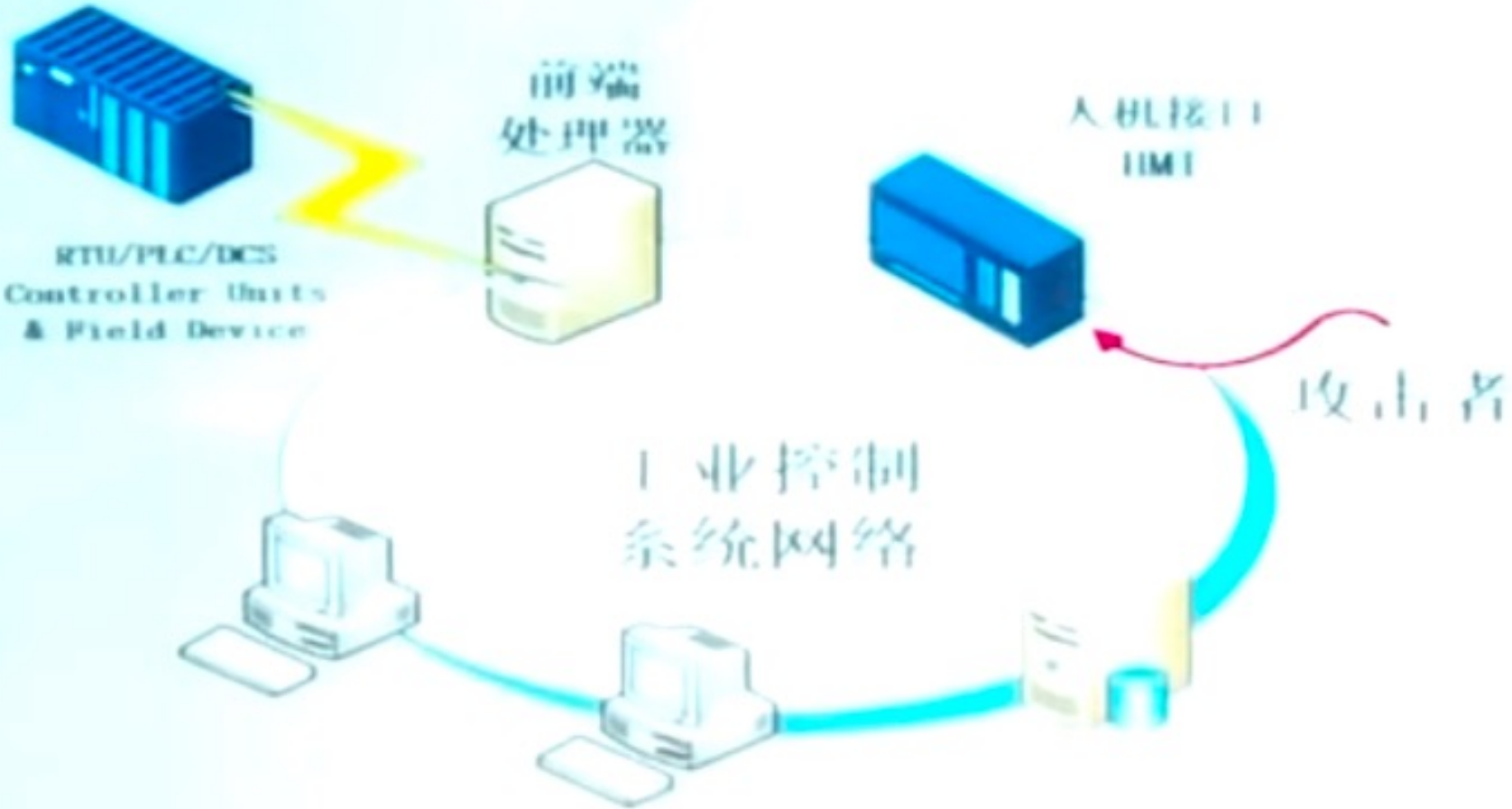
Hack Inn独家整理发布

数据采集设备、控制设备存在可被攻击者直接控制的威胁

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。

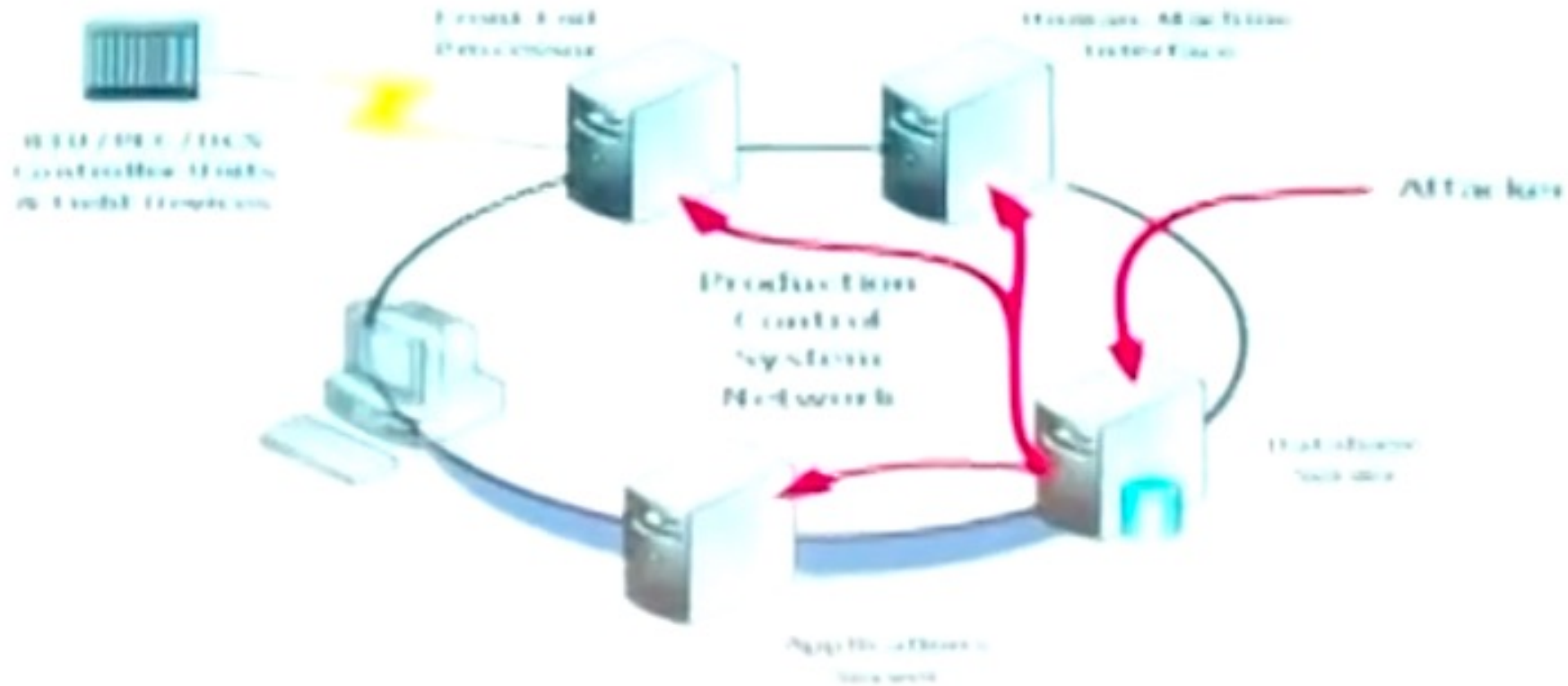
Hack Inn独家整理发布

导出HMI屏幕



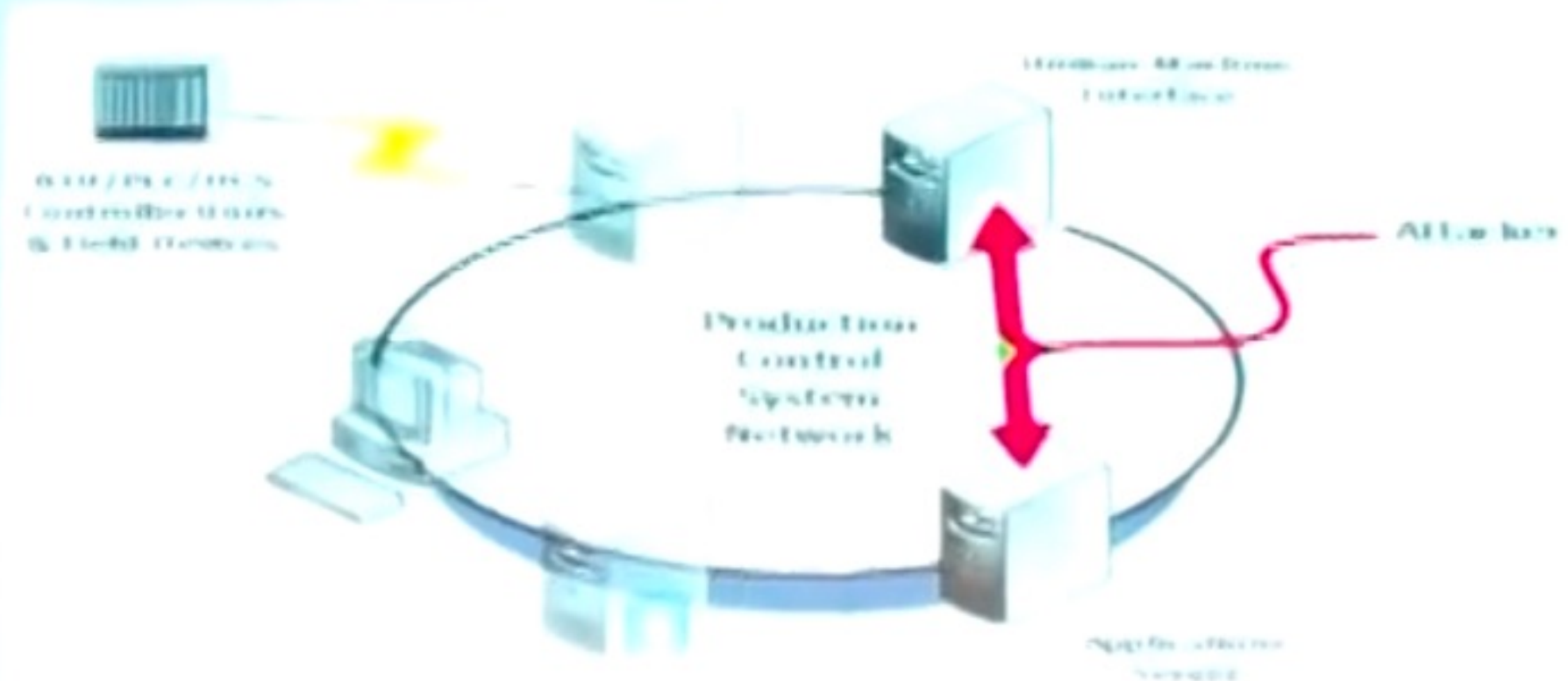
Hack Inn独家整理发布

控制系统数据库的改变



Hack Inn独家整理发布

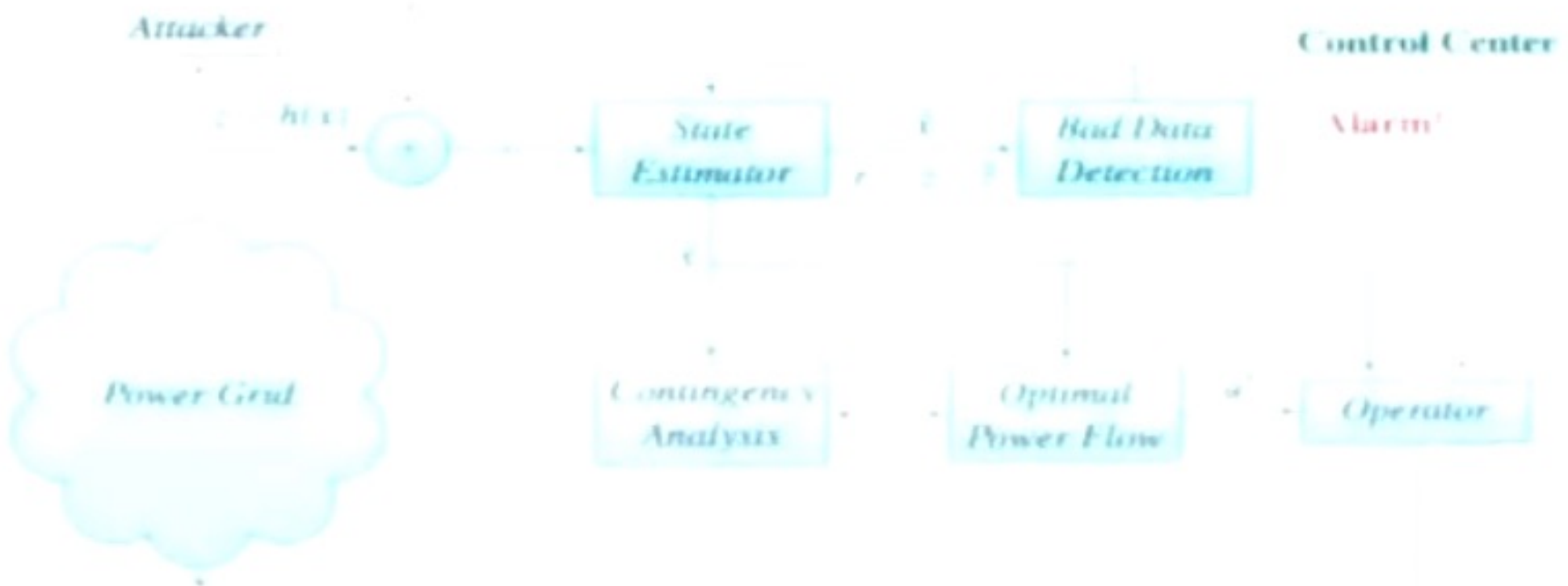
协议存在中间人攻击威胁



通过插入命令到命令流中来实现任意攻击目标命令执行

Hack Inn独家整理发布

错误数据注入攻击威胁



Hack Inn独家整理发布

Hack Inn独家整理发布

1.操作系统漏洞

- 在工控系统中，不同角色运用不同的操作系统，上层工作站基本采用Windows操作系统，中层数据服务器多采用Linux操作系统，底层可编程逻辑控制器以Vxworks操作系统为主。

- 常见的系统提权漏洞、缓冲区溢出漏洞、UPNP漏洞、RDP漏洞等都有可能被攻击者利用，入侵系统，破坏设备，窃取机密信息。

Hack Inn独家整理发布

4.工控设备漏洞

- 工控设备主要包括传感器、测量器、传动装置等IO设备和可编程逻辑控制器(PLC)、智能电子设备(IED)、远程终端控制系统(RTU)等控制设备。

- 常见的这部分漏洞有硬编码凭证漏洞、拒绝服务漏洞、权限绕过漏洞等；

Hack Inn独家整理发布

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

Hack Inn独家整理发布

5.工控协议漏洞

漏洞名称	发布时间	[illegible]	[illegible]	[illegible]
Rockwell Automation MicroLogix 1200 EtherNet/IP协议栈拒绝服务漏洞	2016-02-29	[illegible]	[illegible]	[illegible]
IOServer DNP3协议TCP报文处理拒绝服务漏洞	2013-06-17	[illegible]	[illegible]	[illegible]
RSLinx OPC Automation ActiveX控件栈缓冲区溢出漏洞	2011-06-30	[illegible]	[illegible]	[illegible]

Hack Inn独家整理发布

攻击者的目标和意图

PLC运行时系统

- 1、读工程文件读工程文件
- 2、运行/终止梯形逻辑
- 3、上传梯形逻辑
- 4、下载梯形逻辑
- 5、查看梯形逻辑源码
- 6、改变梯形逻辑代码
- 7、读写总线
- 8、读写进程值
- 9、执行梯形逻辑

文件系统

- 1、读写文件
- 2、读写PLC配置文件
- 3、读写PLC运行时系统文件
- 4、删除文件
- 5、格式化文件系统
- 6、改变文件权限

Hack Inn独家整理发布

PLC恶意代码载荷的生成

- 来自南加州大学的S.McLaughlin的研究
- "On dynamic malware payloads aimed at programmable logic controllers." in HotSec, 2011

Hack Inn独家整理发布

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...
```

Hack Inn独家整理发布

四、现实与展望

工业控制系统防护之难

1

Safety要求高！

2

Update比较困难

3

有限的计算能力

Hack Inn独家整理发布

Seven Steps to Effectively Defend Industrial Control Systems

Seven Strategies to Defend ICSs

Implement Application Whitelisting 38%

Implement Secure Remote Access 1%

Ensure Proper Configuration/Patch Management 29%

Monitor and Respond 2%

Reduce your Attack Surface Area 17%

Manage Authentication 4%

Build a Defendable Environment 9%

Hack Inn独家整理发布

Hack Inn独家整理发布

Hack Inn

一个收集分享国内外安全会议资料的网站，
我们认为每一份议题都值得留传。

https://www.hackinn.com/　　联系邮箱：admin@hackinn.com