Cyber-Physical Systems Security – A Survey

Abdulmalik Humayed, Jingqiang Lin, Fengjun Li, and Bo Luo

报告人：徐梓桑

本文摘要

- 目前缺少对CPS安全问题系统性的研究，特别是使用通用模型的异构或多样性CPS。
- 本文将现有的一些对CPS安全性问题的研究，在统一的框架下进行系统化和分类比较。该框架包括三点：（1）从安全角度来看，本文遵循公认的威胁，漏洞，攻击和控制的分类；（2）从CPS组件的角度来看，本文关注网络部分、物理部分和网络-物理部分；（3）从CPS系统的角度来看，本文探讨一般CPS功能以及其代表性的系统。
- 本文的目的在于构建一个足够抽象的模型，以适用于各种异构CPS的应用。这样能系统性的获得对CPS安全性理解，并突出攻击的潜在来源和保护方式。

本文主要贡献

- （1）本文提出了一个CPS安全框架，用于区分给定系统中的网络部分，网络-物理部分和物理部分。
- （2）本文研究了潜在的威胁源及其攻击动机。
- （3）本文提出了现有的漏洞，并用实际的例子来说明其存在漏洞的根本原因。
- （4）本文研究了一些对CPS的攻击行为，并说明CPS中存在的漏洞对其部件的影响。
- （5）本文还总结了现有的安全控制机制，进一步确定了不同CPS应用中未解决的问题和面临的挑战。

本文主要架构

- 1. 简单介绍了CPS应用中的四个典型系统
- 2. CPS存在的安全威胁与漏洞
- 3. 现存的对CPS的攻击行为
- 4. 控制CPS安全问题的方案
- 5. CPS安全面临的挑战

四个代表性的应用

- 1.工业控制系统（Industrial Control Systems，ICS），ICS是指在工业界，用于加强控制、监测和产能的控制系统，例如核电站，供水和污水系统以及灌溉系统等。其主流的控制器是可编程逻辑控制器（PLC）。ICS的现场设备通过传感器和致动器连接到物理世界。通常，它根据周围环境配置了无线和有线通信。

- 2.智能电网系统（Smart Grid Systems）。智能电网被设想为下一代电网，它已经用于发电、输电和配电几十年了。从国家的角度来看，智能电网能加强对污染物排放的控制，智能发电和节能。从局部角度来看，它使得每家每户能更好地控制其能源的使用。

四个代表性的应用

- 3.医疗设备（Medical Devices）。医疗设备通过融合网络能力和物理能力的方式来改善医疗设备，以提供更好的医疗服务。植入患者体内的设备，称为可植入医疗设备（Implantable Medical Devices，IMD），而由患者佩戴的设备，称为可穿戴设备。 它们通常配备有无线通信能力，以允许与其他设备进行通信。

- 智能汽车（Smart Cars）。 智能汽车是更环保，更节能，更安全，并有着更强娱乐性和便利性的汽车。这些进步是通过50至70个ECU联网而实现的。

四种应用中，CPS的通信技术和协议

- ICS，两个类型的协议，一种用于自动化和控制，例如：Modbus或分布式网络协议（DNP3），另一种用于互连ICS控制中心，例如互通控制中心协议（Inter-Control Center Protocol，ICCP）。以及常用的TCP/IP协议。

- 2.智能电网。类似于ICS，也使用Modbus或DNP3，以及ICCP。但最近使用国际电工委员会（IEC），开发的IEC 61850协议或更高级的协议。而一些现场设备，如智能电表，可能使用短程频率信号，例如Zigbee。

四种应用中，CPS的通信技术和协议

- 医疗设备。医疗设备通常使用无线通信。IMD通常使用低频（LF）信号。可穿戴设备通常使用身体区域网（Body Area Network，BAN）。BAN利用了许多无线通信技术，如蓝牙和ZigBee。

- 智能汽车。本文主要关注车内通信。最常见的协议是（1）本地互连网络（LIN）（2）控制器区域网络（CAN）（3）Flexray，（4）面向媒体的系统传输（MOST）。此外，一些汽车配备了无线连接，如蓝牙和蜂窝接口。

一般CPS威胁模型

- 一般CPS的威胁有以下五个因素：
  - 源
  - 目标
  - 动机
  - 攻击向量
  - 潜在后果

CPS安全威胁

●对ICS的威胁：

- 犯罪攻击（Criminal Attackers）（动机）。熟悉系统的攻击者（源）可以利用无线能力（向量）远程控制ICS应用并可能中断其操作（结果）。

- 经济动机（Financially-motivated customers）（动机）。消费者（源）为了减少对公用事业的支出可能能够通过篡改物理设备或注入虚假数据（向量）的方式，来误导公用事业部门（目标），最终造成其财产损失（结果）。

● 对智能电网的威胁：

- 以犯罪或财政为动机的威胁（动机）。为了闯空门（目标）的小偷（来源）可能能够从智能电表与公用事业公司之间的通信（向量）中推断出屋主的私人信息，例如屋主是否在家，以便入室盗窃（结果）。

CPS安全威胁

●对医疗设备的威胁：

- 间谍威胁（动机）。一个黑客（源）可以使用无线黑客工具（向量），来拦截患者的医疗设备的通信信息，以获得患者的患病情况等隐私信息（目标）。最终，导致患者的隐私被侵犯隐私和信息泄露（后果）。

●对智能汽车的威胁：

- 跟踪威胁（动机）。黑客或执法部门（源）可以利用GPS导航系统（向量）来跟踪汽车（目标），最终导致司机的隐私被侵犯（后果）。

CPS安全漏洞

●造成漏洞的原因：

- 隔离假设（Isolation assumption）。一些系统在设计之初就被假设其系统与外部世界是隔离的。但最近的CPS应用中，越来越不遵守这一隔离假设，导致更多攻击点出现。

- 连接性的增加（Increased connectivity）。现在越来越多的CPS连接上了互联网，导致其更容易被外部攻击。

- 异构性（Heterogeneity）。CPS通常都是由多个不同供应商提供的部件组成。而每个部件都可能存在安全问题。那么，由这些部件组成的CPS就会继承所有部件所存在的安全问题。因此集成之后可能产生不可预计的问题。

●本文将漏洞分为三种：网络漏洞，网络-物理漏洞和物理漏洞。下面将根据四个代表性应用进行说明。

网络漏洞

ICS漏洞：

- 网络部分中的通信漏洞（Communication vulnerabilities in cyber components）。有线部分，ICS对TCP/IP协议的依赖性在增加，而TCP/IP协议仍然存在安全性问题。另一种协议是远程过程调用（Remote Procedure Call，RPC），其也具有许多安全漏洞，其中之一导致了众所周知的Stuxnet攻击。此外，互连控制中心协议（ICCP）也缺少诸如加密和认证的基本安全措施。
- 无线部分，ICS的短距离无线通信可以被内部人员捕获，分析或操纵。或者内部员工将其自己的不安全的设备连接到ICS无线网络，导致整个网络暴露在潜在的威胁中，使得攻击者可以使用这些设备作为攻击媒介。蜂窝，微波和卫星等通信方式，通常用在ICS的远距离无线通信中。目前尚未有无线通信中的漏洞对ICS的影响的研究。
- 软件漏洞（Software vulnerabilities）。目前，主流的网络相关漏洞是SQL注入（A popular web-related vulnerability is SQL injection），攻击者可以在没有授权的情况下访问数据库的记录。此外，电子邮件也有助于恶意软件扩散到网络。

网络漏洞

智能电网漏洞：

- 网络部分中的通信漏洞。智能电网的信息基础设施依赖于许多具有已知漏洞的标准化互联网协议，可用于对电网发起攻击。例如TCP/IP协议，它不应该被连接到控制中心。此外，用于控制中心之间交换数据的标准协议ICCP（Inter-Control Center Protocol），存在一个缓冲区溢出的严重漏洞。

- 软件漏洞。与ICS类似。例如，广泛应用的可远程升级的智能仪表，是一个容易招致攻击的部件。攻击者可以利用其中存在的漏洞，来控制该仪表甚至是控制中心，最终引起大规模停电。

- 隐私漏洞。由于客户住宅的智能仪表和公用事业公司之间可进行双向通信，这导致出现了一种新型的漏洞。攻击者可能能够拦截从智能电表产生的大量流量并推断关于客户的私人信息。例如，户主的日常习惯或户主是否在家。

网络漏洞

医疗设备漏洞：

- 安全性定义不清晰（Security through obscurity）。由于缺乏对医疗设备制造商的强制性安全标准，使得大部分现有的医疗设备都是由个人设计的专有协议并将其作为安全措施，而这种措施往往都无法阻止攻击者。

- 网络部分中的通信漏洞。由于大多数医疗设备依赖于无线通信，这意味着设备易受到一系列基于无线的攻击，例如干扰，噪声，窃听，重放和注入攻击。

- 软件漏洞。软件的作用在医疗设备中一直在增长，因此具有存在软件漏洞的可能性。由于软件存在缺陷而导致的设备故障可能会危及健康状况。

网络漏洞

智能汽车漏洞：

- 网络部分中的通信漏洞。例如，通过蜂窝数据接口窃取车辆的GPS数据，以获得车辆的行踪等隐私信息；又或者通过车内麦克风，窃取车内人员谈话的隐私信息。蓝牙是智能车中最易受攻击的载体之一。 当乘客想要将电话与汽车配对时，唯一的认证措施是由汽车的远程信息处理控制单元（TCU）提示的个人识别号（PIN）。但这个措施是不够的，攻击者可以通过欺骗蓝牙的软件暴力破解PIN，拦截，甚至注入假PIN。

- 软件漏洞。软件是每个ECU的核心，智能汽车对它的依赖显着增加。这反过来增加了软件存在缺陷和安全漏洞的可能性。例如，媒体播放器具有直接连接到CAN总线的能力。这意味着播放器中存在的漏洞可能可以影响到其他ECU的运行。

网络-物理漏洞

ICS漏洞：

- ICS组件之间的通信（Communication between ICS components）。ICS依赖于专有的协议，如Modbus和DNP3，其用于监控和发送控制命令。ModBus协议缺乏基本的安全措施，因此很容易受到攻击。例如，缺乏加密措施，缺乏数据完整性检查。DNP3协议也没有任何类型的加密或认证机制。
- 操作系统漏洞（OS vulnerabilities）。ICS设备（例如PLC和RTU）中的操作系统是实时操作系统（RTOS），并且它们不实施访问控制措施。因此，所有用户都被赋予最高的权限，即根访问权限。这是不安全的，设备很容易招致各种攻击。
- 软件漏洞（Software vulnerabilities）。我们将在通用操作系统上运行的，用于控制和监视控制器的程序视为网络物理组件。PLC和其他现场设备具有有限的计算能力，并且不能执行计算昂贵的解决方案，例如加密措施。因此，很容易受到攻击。

网络-物理漏洞

智能电网漏洞：

- 电网通信漏洞（Grid communication vulnerabilities）。与ICS类似，采用几乎相同的协议，例如Modbus和DNP3，因此其存在的漏洞与ICS一致。此外，最近还引入了更先进的IEC 61850协议，但该协议中的安全性依旧不足。例如，该协议缺少加密措施，使得传输中的数据易于被窃听，这很容易招致被攻击。

- 智能电表的漏洞（Vulnerabilities with smart meters）。智能仪表依赖于双向通信，这导致了许多新的安全问题，攻击者可以利用这种交互的能力。例如，智能电表可以具有攻击者可以利用的后门，以完全控制该设备。

网络-物理漏洞

医疗设备漏洞：

- 网络-物理组件中的通信漏洞（Communication vulnerabilities in cyber-physical components）。可穿戴设备和IMD中的无线通信是存在漏洞的，而这些漏洞被利用时，可能会对患者造成物理性质的影响。同时，由于设备依赖于无线通信，也存在出现干扰攻击的可能性。例如，通过重放攻击，使设备进行大量运算以耗尽设备电池。

- 设备认证（Device authentication）。攻击者可以使用未经认证的商用编程器作为可信赖的一个编程器。一些攻击甚至不需要编译器，其通过软件无线电外围设备（Universal Software Radio Peripheral ，USRP）就足以替代编程器并且发送恶意数据包。

网络-物理漏洞

智能汽车漏洞：

- 网络-物理组件中的通信漏洞。车载通信协议，如CAN和LIN，缺乏加密，身份验证和授权机制。由于缺乏加密，TPMS容易受到窃听和欺骗。

- 提高舒适性的ECU（Comfort ECUs）。例如，自适应巡航控制（ACC），车道保持辅助，碰撞预防等ECU。这些组件是CAN网络的一部分，因此，可以利用这些ECU的漏洞来进入CAN网络，以攻击其它的ECU。

- X-by-wire的漏洞（Vulnerabilities with X-by-wire）。智能汽车的一个新兴趋势是“X-by-wire”。其目的是通过电子或机电部件逐渐替代汽车中的机械控制部件，例如方向盘和制动踏板。这意味着攻击者可以利用这些新功能发动网络物理攻击。该技术依赖于FlexRay通信协议，其在速度和安全特性方面比CAN协议更先进。但由于成本高昂，不太可能很快在市面上普及。

物理漏洞

- CPS文献中的大多数漏洞分析集中在网络攻击对物理的影响（cyber attacks with physical impact），而研究物理攻击对网络的影响（physical attacks with cyber impact）的很少。
- ICS漏洞:
- 许多ICS组件，如远程终端和PLC，本身就是一个漏洞。由于提供给这些组件的物理安全性不足，它们很容易受物理篡改甚至破坏。例如，水渠的传感器依靠太阳能电池板作为能量源，若这些面板被盗，则会导致控制中心无法接收到该水渠的传感器数据。
- 智能电网漏洞：
- 与ICS类似，智能电网的现场设备直接被置于不受保护的环境中，因此易受到直接物理破坏。例如输电线被破坏等。此外，连接到建筑物，房屋和偏远地区的智能电表也使它们容易成为各种物理攻击的目标。

物理漏洞

- 医疗设备漏洞:
  - 无论是可植入的还是可穿戴的医疗设备，都有可能受到物理访问。例如，出于维护目的，攻击者利用设备所有者警惕性的缺乏，篡改它并且可能执行恶意活动，例如恶意软件安装或修改配置，使得设备传递可能威胁患者健康的未经修改的治疗。而另一个漏洞是医疗设备用户的移动性。由于设备的设计者不能控制患者的周围环境，当患者处于不安全的位置时，设备可能受到不可预测的物理攻击。

- 智能汽车漏洞：
  - 如果没有物理保护，汽车可能容易受到许多攻击。 例如，TPMS部件可能被破坏，导致DoS攻击，使得TPMS不能将轮胎的空气压力发送到指定的ECU。此外，将暴露汽车的物理访问端口是另一个可能导致严重攻击的漏洞。 例如，机械师可以通过OBD-II端口直接访问汽车的内部部件。

- 综合图见论文

当前存在的CPS攻击

- 本文基于被损害的位置，将攻击分为了三类：
- 网络攻击：没有到达传感器/执行器的攻击。
- 物理攻击：直接影响物理组件的攻击。
- 网络-物理攻击：通过网络组件间接影响物理组件的攻击。

网络攻击

ICS攻击：

- 通信协议（Communication protocols）。许多攻击利用了通信协议中的漏洞。
- 间谍（Espionage）。例如Flame病毒。其瞄准中东的各种ICS网络，并在2012年被发现。这种恶意软件的主要目标是收集公司的私人数据，如电子邮件，键盘敲击和网络流量。此外，在2013年，一群被称为蜻蜓的黑客，针对美国和欧洲的能源公司发动了攻击。攻击者的主要目标似乎是收集私人信息。
- 无意攻击（Unintentional attack）。 虽然更新软件对于减少系统中的漏洞是至关重要的，但它可能是服务中断的来源。 例如，在核电站中，控制中心中的一台计算机被更新并随后重新启动。 重新启动删除控制系统上的关键数据。当数据被擦除时，系统的其他部件误解这种损失，导致操作和设备关闭的异常。
- 基于Web的攻击（Web-based attacks）。夜龙攻击（Night Dragon attack），2011年，针对敏感信息从私人网络的一些能源和石油公司。攻击采用了很多方法，如SQL注入漏洞和恶意软件注入。

网络攻击

智能电网攻击：

- DoS。对于智能电网来说，数据的实时性是至关重要的，数据延时可能造成无法估计的后果。而DoS攻击几乎充斥着网络的所有层面。

- 错误数据注入（False data injection）。 在智能电网中引入虚假数据会导致不同的后果，例如服务中断和资金损失。

- 用户信息（Customers’ information）。攻击者可以分析智能电表和数据中心之间的智能电网中的网络流量，以推断关于用户的私人信息。例如，攻击者可以确定目标在特定时间是否在家。

- 无目标的恶意软件（Untargeted malware）。2003年，Slammer蠕虫导致了禁用现场设备和变电站之间的流量。虽然恶意软件不打算影响能源部门，但由于智能电网网络的互联性，它仍然有效。 恶意软件消耗了大量的时间关键流量，但没有导致服务中断。

网络攻击

医疗设备攻击：

- 虽然大部分的攻击已经在实验室环境中进行测试了，但本节所说的希望可以刺激提高医疗设备的安全性。虽然一些攻击是特定于某些设备，例如胰岛素泵，但是相同的攻击技术可以应用于其他IMD和可穿戴设备。

- 重放攻击（Replay attacks）。通过利用胰岛素泵中的漏洞，可以通过结合先前拦截的设备的PIN来重放被窃听的分组。此外，重放攻击可能导致关于胰岛素注射的错误的决定。

- 侵犯隐私（Privacy invasion）。侵犯患者隐私的攻击有不同的目标和后果。例如，对于文献[91]中对胰岛素泵的远程控制攻击，攻击者需要了解从遥控器发送的设备类型，PIN和合法命令。

网络攻击

智能汽车攻击：

- 目前大部分对智能汽车的安全性研究都是比较抽象的，只有很少一部分是在真车上做了实际实验的。为了成功攻击汽车，攻击者需要通过OBD-II端口，媒体播放器或USB端口，或通过蓝牙或蜂窝接口无线地访问内部网络。 一旦攻击者进入汽车的内部网络，大量的攻击机会就会开放。

- DoS。DoS攻击可以采取不同的形式，其影响在安全关键性上变化。例如，在巡航时，驾驶员增加速度，但仪表盘上不改变，这将达到一个危险的速度。

- 虚假数据注入（False Data Injection，FDI）。这种攻击的一个例子是在速度计上显示假速度。攻击者首先拦截由BCM发送的实际速度更新分组，然后发送具有假速度的修改分组。或者修改安全气囊状态等。

- 侵犯隐私（Privacy invasion）。 Checkoway等人[18]能够利用TCU中的蜂窝接口并在车内对话中窃听。

网络-物理攻击

ICS攻击：

- 传统通信渠道（Legacy communication channels）。拨号连接提供对现场设备的直接访问，并且有时其安全性被忽略。在2005年，有人通过利用运河系统中的拨号连接访问了水利设施的计费信息。

- 心怀不满的内部人员（Disgruntled insiders）。2000年，一名雇员故意打乱澳大利亚昆士兰州Maroochy水务局污水处理系统的运作。攻击者利用他的知识，以及作为一个前合法的内部人员身份，使用笔记本电脑和无线电发射器改变泵站的配置。攻击的后果造成大量的原污水涌入街道，污染环境。

- Modbus蠕虫（Modbus worm）。Fovino等人[116]制作了利用Modbus协议中缺少身份验证和完整性漏洞的恶意软件。该蠕虫旨在执行两种攻击：DoS，通过识别传感器或执行器，并通过向传感器或执行器发送未授权命令来发送DoS诱导消息和命令注入。

网络-物理攻击

- 恶意软件（Malware）。一些恶意软件针对特定系统实现目标，如流量拦截和操作中断。它们利用管理控制现场设备的应用程序中的软件漏洞。一个着名的例子是Stuxnet。

- 基于Web的攻击（Web-based attacks）。一些黑客利用了一个基于Web的界面直接连接到了现场设备（如PLC）。他们不断地打开这个连接直到授权用户无法访问该设备，从而导致了DoS攻击。此外，他们还向控制器或现场设备发送了一个网页，其中包含恶意Java脚本代码，旨在利用TCP/IP堆栈中的错误，导致控制器重置。

网络-物理攻击

智能电网攻击：

- 网络勒索（Cyber extortion）。这种类型的攻击比较罕见，但至少是公开性质的，攻击者控制目标智能电网，并以不造成大规模停电为代价提出一些要求。

- 停电（Blackouts）。停电在智能电网中被认为是DoS攻击。保证智能电网的可用性可能是最重要的安全目标。2007年，爱达荷国家实验室（INL）展示了一个关于如何通过网络攻击破坏发电机的实验。实验证明了这种攻击的可行性。

网络-物理攻击

医疗设备攻击：

- DoS攻击。当DoS攻击成功时，可能导致患者的严重健康状况。例如发送了“关闭”命令来禁用ICD。

- 虚假数据和未授权的命令注入（False data and unauthorized commands injection）。 Li等人[91]能够远程控制胰岛素泵的遥控器，并成功停止并从20米距离处恢复胰岛素注射。

- 重放攻击（Replay attacks）。通过利用重放攻击对策中的软件漏洞，任何数据包都可以重传到CGM和胰岛素泵

网络-物理攻击

智能汽车攻击：

- DoS。DoS攻击的一种形式是攻击者阻止乘客关闭任何打开的窗户。另一个是禁用警告灯或盗窃报警系统，使得汽车不能在需要时产生警告和警报。此外，无线通信的干扰也是DoS的一种形式，例如干扰RKE信号。

- 通过蓝牙进行恶意软件注入（Malware injection via Bluetooth）。恶意软件通过蓝牙连接，然后向TCU发送恶意数据。一旦TCU被攻破，攻击者可以与控制安全部分的ECU通信，如防抱死制动系统（ABS）。

- 通过蜂窝网络注入恶意软件（Malware injection via cellular network）。恶意软件可以利用TCU中的蜂窝信道对智能汽车发起注入攻击。攻击通过播放MP3文件注入有效信息来实现。

网络-物理攻击

- 通过OBD-II端口注入恶意软件（Malware injection via the OBD-II port）。通过OBD-II端口的恶意软件注入需要物理访问汽车。

- 数据包注入（Packet injection）。此攻击需要先取得CAN网络的访问权。一旦攻击者以物理或无线方式进入网络，就可能发生大量攻击。例如，通过OBD-II端口，可以增加引擎的每分钟转数（RPM），干扰引擎的计时，禁用发动机，干扰刹车等。

- 重放攻击（Replay attacks）。该攻击需要两个步骤：1）当某些功能被激活时拦截CAN网络业务，以及2）重传观察到的分组以重新激活相同的功能。

物理攻击

ICS攻击：

- 无目标攻击（Untargeted attacks）。Zotob蠕虫的目标虽然并不是ICS，但其能导致工厂停工。例如，美国戴姆勒-克莱斯勒不得不关闭其13个制造工厂大约一个小时。这样的事件激发研究人员检查用于传统IT系统的意外恶意软件对ICS网络的影响。

物理攻击

智能电网攻击：

- 自然和环境事件（Natural and environmental incidents）。在2014年，由于自然原因以及智能电网中的一些不可靠的组件影响，造成了大规模停电事故。费城的一场暴风雪造成了影响75万人数天时间的大规模停电事件。

- 盗窃（Theft）。对于小偷来说，盗窃铜线和金属设备是有利可图的。例如，在西弗吉尼亚州曾因盗窃问题造成了影响3000人的停电。

- 车祸（Car accidents）。在2014年，美国有356起停电是由于汽车撞击输电塔，变压器或电线杆而造成的。

- 故意破坏（Vandalism）。攻击者可以采用物理损坏的方式破坏智能电网的部件，如电缆，电线杆，发电机，智能电表和变压器。

- 恐怖袭击。2014年，也门发生了第一次对电网的恐怖袭击。袭击者发射火箭以摧毁输电塔，造成全国停电，影响到2400万人。

物理攻击

医疗设备攻击：

- 获取唯一ID（Acquiring unique IDs）。要攻击目标设备，获取该设备的序列号是前提条件。

智能汽车攻击：

- 中继攻击（Relay attacks）。捕捉钥匙发送的“开门”超高频（UHF）信号，然后克隆出一个汽车钥匙，用其来开启汽车门。

- ABS欺骗（ABS Spoofing）。由于测量车轮速度的传感器原理是测量有车轮转动引起的磁场改变，Shoukry等人[141]在所示的攻击中，介绍了产生另一个磁场的恶意致动器，其中断了由车轮速度传感器产生的原始场。导致ABS的ECU接收不到正确的数据，使其测量不准确。

- 各类型综合见论文表2、3、4

一般CPS控制方案

- 控制更多的连接（Controls against more connectivity）。比较考虑到一些新的安全注意事项，以确保接入点免受未经授权的访问。此外，通信协议既不能是专有协议，例如部署的ICS和智能电网中的Modbus和DNP3，也不能是诸如TCP / IP的开放协议。因为在设计这些专有协议时，存在隔离假设，这导致其存在大量漏洞。
- 通信控制（Communication controls）。ICS通信层面的安全解决方案应考虑与传统IT解决方案的差异。例如，入侵检测系统（Intrusion Detection Systems，IDS）应该是时间关键(time-critica)的，因此长延迟是不能容忍的.
- 设备认证(Device Attestation）。在CPS组件中运行的软件需要验证其真实性。此验证有助于显着减少恶意软件。例如，基于硬件的解决方案诸如可信平台模块（Trusted Platform Module，TPM）可以提供代码进行验证。然而，TPM被假定为物理安全的，这在一些CPS应用（例如ICS和智能电网）中是不可能的。TPM的另一个问题是，在CPS应用中的计算资源是有限的。

特定系统的控制方案

ICS控制方案：

- 全新的设计（New design）。ICS需要专门为其设计一套安全解决方案。这些解决方案应考虑网络-物理相互作用以及组件和协议的异构性。目前大多数的ICS解决方案旨在提供可靠性，但目前需要同时考虑安全性与可靠性。

- 具有附加安全性的协议（Protocols with add-on security）。ICS通信层面的安全解决方案应与传统IT解决方案有着根本的区别。许多提案依赖于对当前协议的修改，如Modbus，DNP和ICCP，以集成安全性。

- 入侵检测系统（Intrusion Detection Systems，IDS）。设计用于保护ICS的IDS的复杂性比在传统IT安全中相对较少。这是由于网络的流量和静态拓扑的可预测性。
- 远程访问现场设备（Remote access to field devices）。Fernandez等人[41]建议只有经授权的人员才能远程访问现场设备。访问应通过使用指定的笔记本电脑通过VPN严格保护。关闭空闲连接。或者禁止同时多个连接。

特定系统的控制方案

- 加密和密钥管理（Encryption and key management）。加密带来的相关问题之一是延迟，而延迟在时间敏感（time-sensitive）的环境中，延时是不被希望出现的。Choi等人[27]提出了一种ICS特有的密钥管理解决方案，不会造成延迟。

- 软件控制（Software controls）。定期对操作系统及应用程序打补丁以减少漏洞是非常重要的。Windows发布了Stuxnet相关的安全补丁，没有它，Stuxnet仍然存在。

- 标准化（Standardization）。国家标准与技术研究所（The National Institute of Standards and Technology，NIST）是标准化领域的领先机构之一。遵循他们的ICS安全标准能显着的提高ICS安全性。

特定系统的控制方案

智能电网控制方案：

- DoS控制（DoS controls）。应防止或至少检测到对通信组件的攻击。在网络层，通常通过限速，过滤恶意数据包和重新配置网络架构来实现DoS等攻击防范。

- 入侵检测系统（Intrusion Detection Systems，IDS）。智能电网的IDS设计还处于不成熟的阶段。由于电网的规模十分庞大以及其组成部件的异构性，导致设计智能电网的IDS是一项十分复杂的任务。

- 低级别的授权和认证（Low-level authorization and authentication）。在诸如智能电网的大型系统中，常见的问题是对需要访问低级层设备（例如现场设备）的用户的认证和授权。通常情况下，所有的现场设备共用一个密码，并且该密码已告知给所有员工，这就不可避免的存在安全隐患。一个心怀恶意的员工可以对现场设备进行一些恶意改变，事后也无法追查是何人所为。

特定系统的控制方案

- 全新的设计（New designs）。随着技术的发展，新的安全问题层出不穷，这需要对智能电网的方方面面采取不同的方式来保证其安全。不光网络部分，网络-物理部分也需要被考虑在内。
- 安全扩展（Security extensions）。智能电网的各个部件的安全性都在不断增加。如DNP3，IEC 61850和IEC 62351协议被扩展以获得安全属性。
- 隐私保护控制（Privacy-preserving controls）。缺乏保密性的数据聚合协议（data aggregation protocols）可能导致消费者的私人信息被侵犯，例如计费信息和使用模式，而缺乏完整性可能导致状态估计和消费报告（state estimation and consumption reports）的中断。因此，数据在智能仪表和控制中心之间传输时，必须使用隐私保护技术，以提供具有保密性和完整性的聚合数据。另一个隐私的关注点可能影响到生命和财产安全，那就是检测房屋内是否有人，以便犯罪分子闯空门。
- 标准化（Standardization）。许多机构，如IEC和NIST，已经制定了一套用于确保智能电网通信的标准。例如，IEC已制定标准TC57和6235，而NIST已在报告7628中制定了智能电网指南。

特定系统的控制方案

- 智能仪表禁用预防（Smart meters’ disabling prevention）。为了防止远程攻击者利用智能仪表中的禁用功能，Anderson和Fuloria [4]建议智能仪表应该被编程为在“禁用”命令生效之前提前通知客户，之后再禁用仪表。此措施有助于在DoS尝试发生之前及早发现。

- 物理安全（Physical security）。由于智能电表是物理暴露的，因此必须对其进行物理保护。NIST标准指出，除了物理保护之外，智能电表必须具有加密模块。这些标准还强调需要将智能仪表密封在防篡改单元中，使得未授权方不能对其进行物理篡改。

特定系统的控制方案

医疗设备控制方案：

- 验证（Authentication）。Halperin等人[56]提出了一种基于密码的认证和密钥交换机制，以防止未经授权的设备访问IMD。这两种机制不以电池作为能量源。相反，它们依赖于外部射频。此外，带外（Out-of-Band，OBB）认证被部署在一些可穿戴和可植入设备中。
- 入侵检测系统（Intrusion Detection Systems）。Gollakota等人 [51]提出了Shield，其能检测和防止对IMD基于无线的恶意攻击。在设计IDS时，需要考虑植入和可穿戴设备的独特属性，它们与独立的医疗装置，例如生命体征监测器和心脏装置，是不同的。
- 基于位置的控制（Location-based controls）。一些解决方案使用在通信设备间是基于物理距离的远程协议，这样一来，远程攻击者就不能发动远程攻击。该距离由诸如超声信号，接收信号强度（received signal strength，RSS），心电图（electrocardiography，ECG）信号和身体耦合通信（bodycoupled communication，BCC）等技术决定。但此技术只提供认证，不提供授权。因此，还需要纳入其他技术。

特定系统的控制方案

- 瓦解主动和被动攻击（Thwarting active and passive attacks）。Li等人[91]提议使用身体耦合通信（bodycoupled communication，BCC）。这是因为BCC依赖于人体作为传输介质，而以空气为传输介质的通信是很容易被拦截的。当人体成为传输介质时，攻击者需要非常接近患者，甚至与直接身体接触。这显然能减少攻击，为攻击者提高了攻击难度。
- 将安全转移到可穿戴设备（Shifting security to wearable devices）。将安全结合到现有的IMD和可穿戴设备存在很大的风险和挑战。其中之一便是通过手术将老旧IMD替换为安全性更高的IMD。就算提取IMD没有任何风险，但用于安全体系所需的加密解密运算等，会占用大量IMD的存储器空间以及消耗大量电池电量。因此，直观的解决方案是添加专门为增加安全性而构建的另一个设备。这些设备可以利用外部穿戴设备来实现。
- 跨域解决方案（Cross-domain solutions）。Li等人[91]提出采用用于汽车中的RKE的滚动码加密机制。智能汽车和医疗设备在计算限制，功率和数据带宽限制方面都具有类似的特征。 因此，使用滚动码加密应该是防止窃听和重放攻击的有效解决方案。

特定系统的控制方案

- 标准化和建议（Standardization and recommendations）。食品和药物管理局（The Food and Drug Administration，FDA）是医疗器械标准化的领先机构。它已经为医疗设备制造商颁布了一些标准和指南。例如，2014年发布了一项有关医疗设备网络安全的建议。然而，该建议不够详细，也不强制实施，属于“不具约束力的建议”。因此，制造商有自由选择不采纳这些建议，这肯定会导致生产出一些不太安全的医疗设备。

- 允许还是不允许远程功能（Allowing vs. disallowing remote functionalities）。为了防止攻击者渗透医师与患者设备之间进行交互的网络，制造商应禁止通过网络发送远程数据的能力。他们只允许远程方接收措施和日志，但不允许发送命令。虽然这是一个很好的安全做法，可以防止攻击者发送远程命令，但它限制了此类设备的部分功能。因此，需要在安全性和可用性之间取得平衡，而不对患者造成远程威胁。

特定系统的控制方案

智能汽车控制方案：

- 尚未实现但有希望实现（更有效）的控制（Unimplemented promising controls.）。目前已经提出了许多安全控制方法来保护车内网络，但其中的大部分还没有被实现。例如，Wolf等人[162]提出了三个控制来保护总线网络：认证网关，加密和防火墙。
- 加密（Cryptography）。使用加密能大幅提高汽车的安全性。但在汽车这种计算资源有限的情况下融合加密功能，其实现的代价很高昂。因此，部署高效的解决方案至关重要。Wolf等人[161]和Escherich等人[39]提出了专为汽车安全设计的基于硬件的解决方案。
- 重新定义信任的定义（Redefining trust）。Koscher等人[80]建议两个信任相关的控制方案（suggest two trust-related controls），该方案将阻止大多数攻击。首先，撤销对每个ECU的信任，使其不能执行诊断和重新刷新操作。其次，具有诊断和重新刷新功能的ECU必须在执行这些任务之前得到授权和认证。

特定系统的控制方案

- 关键命令受到限制（Restricted critical commands）。 Koscher等人[80]认为在合法部件（legitimate parties）发出“危险”命令之前，应该通过物理层获得访问。但这也可能会引起在某一个部件中的正常指令，却引起另一个部件发生异常的情况。同时，如果制造商决定通过物理访问来限制大量的命令，这将导致其灵活性和便捷性会受到影响。

- 蓝牙（Bluetooth）。设备和汽车之间的蓝牙连接可以被利用以发动各种攻击。汽车需要一个额外的安全层来防御依赖于蓝牙的攻击。
- 入侵检测系统（IDS）。大多数的IDS是为CAN协议设计的，只有少数用于其他协议，如FlexRay和LIN。因此，也需要对FlexRay和LIN等协议设计一套IDS。

- 物理攻击控制（Physical Attacks Controls）。Shoukry等人[142]提出了一种在物理层工作的挑战-响应认证（challenge-response authentication）方案。该方案能检测和防止一些物理攻击，如传感器欺骗。该方案利用物理/模拟域中的信号的物理性质来实现它们的方案。

CPS安全面临的挑战

一般CPS面临的挑战：

- 安全设计（Security by design）。在大多数CPS的设计中，由于其隔离在物理安全环境中，并且没有连接到其他网络（例如因特网），因此不考虑安全其安全问题。因此，物理安全几乎是主要的安全措施
- 网络物理安全（Cyber-physical security）。CPS的设计者需要同时考虑物理方面和网络方面，这样才能更好的预测到由网络攻击而引起的物理后果，并且减少这样的事件发生。此外，被攻击系统的生存能力在CPS中也是非常关键的。
- 实时性本质（The real-timeliness nature）。在CPS受到攻击时，CPS的实时性决策对系统的生存性至关重要。因此，在CPS安全性设计中，同时考虑整个系统的物理和网络方面，能有助于设计更好的风险评估，攻击检测和攻击弹性（attack-resilient）的解决方案。此外，加密机制可能会导致延迟，这可能会影响某些实时系统的性能。因此，应考虑轻量级和基于硬件的加密机制。

CPS安全面临的挑战

- 不协调的变化（Uncoordinated Change）。与CPS利益相关的人相对较大。这包括制造商，实施者，运营商，管理员和消费者。他们的扮演的角色和权限有所不同，因此需要妥善管理。当一个CPS的部件发生变化时，利益相关者在某种程度上需要进行一些协调。例如替换硬件，更新软件，加入新功能等。任何不协调的变化可能改变关于CPS安全性的初始假设，因此可能引入新的漏洞。

CPS安全面临的挑战

ICS面临的挑战：

- 变更管理方式（Change management）。遍布各地的ICS，都可能需要在某一时刻进行更换，更新或移除各种系统。例如，在ICS中，系统更新需要仔细规划，以避免由于工厂的业务网络中的计算机的更新而在导致核电站中发生意外故障。因此，应引入某种协调变化管理，以防止和检测ICS应用中的安全相关变化。

- 内部威胁（Insider threat）。这可能是防御的最困难的威胁之一。内部人员可能会故意或无意造成安全问题。例如，内部人员可以利用给予他的信任以及获得的内部知识来发起攻击。

- 安全集成（Secure integration）。由于ICS严重依赖传统系统，因此它也存在传统系统的漏洞。因此，新组件与传统系统的集成必须安全地进行，以便不会导致新的安全漏洞。此外，由于ICS中存在大量的传统组件，从经济角度上看，一次性用更安全的组件来替换所有的传统组件是不可能的。

CPS安全面临的挑战

智能电网面临的挑战：

- 双向通信（Two-way communication）。智能电网的一个显着特点是双向通信，这得益于先进的计量基础设施（advanced metering infrastructure，AMI）。与电网不同，AMI允许连接到消费者家中的智能电表，而这些电表很容易被物理攻击者访问，并与公用事业公司进行通信。

- 访问控制机制（Access control mechanisms）。由于智能电网存在巨大地理覆盖面，再加上大量的利益相关者，导致智能电网必须要有一个适当的访问控制机制。

- 隐私问题（Privacy concerns）。由于消费者的数据已经成为智能电网通信数据中的重要组成部分，因此，隐私问题已成为一个巨大的挑战。不仅应该对消费者的数据进行加密，而且还需要使用匿名化技术来防止第三方通过推理和其他攻击方式，从加密数据中推导出模式以获得私人信息。

CPS安全面临的挑战

- 显式信任（Explicit trust）。敏感数据和发送的命令不应采用显式信任。相反，我们需要一套新的机制来检测虚假数据和未经授权的命令。

- 综合性安全（Comprehensive security）。安全的防范措施和防范工具主要存在于智能电网的较高层级，而在较低层级的有效性大为降低。在较低层实施安全性可能会导致成本增加，而加密方案又是必不可少的。因此，需要采用轻量级解决方案，则其面临的挑战不是如何部署它，而是如何降低组件的的成本。

- 变更管理方式（Change management）。变更管理智能电网中的管理方式所带来的的挑战并不比变更ICS中的少。智能电网肯定比ICS应用更多样化，拥有更多的利益相关者，但其变更管理方式能力有限。

CPS安全面临的挑战

医疗设备面临的挑战：

- 安全性还是可用性（Security vs. Usability）。过于安全可能导致当患者处于紧急情况时，设备无法被重新配置。例如，一个配有IMD的患者可能处于需要被紧急处理的情况中，但在场的是另一个健康护理提供商。而此提供商没有加密凭证或访问权限来允许他/她重新配置IMD，因此IMD的不可用性可能导致患者处于非常危险情形中。因此，设计中应当在可用性和安全性之间找到平衡点，使得可用性在紧急情况下得以使用。
- 附加安全≈增加代码（Add-on security ≈ increased code）。将安全性直接添加到IMD可能增加代码的大小，从而导致医疗设备召回率的提升。此外，加密操作还会影响整个医疗设备的有限的功率。因此，IMD的功能应该限制于纯医疗操作并将安全服务转移到外部设备。
- 有限的资源（Limited resources）。加密机制通常需要消耗大量计算功率，而这些功率在IMD等设备中属于关键资源。根据设备的不同性质，其至少要能保证设备正常运行多年。对于需要放置到患者体内的手术的装置，它们必须能够至少运行十年或两十年。

CPS安全面临的挑战

智能汽车面临的挑战：

- 安全集成（Secure integration）。不兼容的安全假设（Incompatible security assumptions）通常发生在，当制造商将COTS和第三方组件集成到智能车中时。通常导致这种不匹配的原因是缺乏产品的内部细节。因此，制造商需要确保COTS和第三方组件的安全集成。

- 有效分离（Effective separation）。虽然网关ECU能将CAN网络流量分离为高带宽和低带宽，但许多攻击手段都能够绕过它并获得受到限制的带宽访问。一个有希望的解决方案是使用以太网/IP通信和用Master-ECU替换网关ECU 。一方面，这可以提供更大的带宽，因此加密解决方案可以在不增加通信开销的情况下工作，并且能达到更高的运行速度。另一方面，它要求制造商更换传统的ECU和网络体系结构，而这项工作需要花费高昂的代价。

CPS安全面临的挑战

- 部件的异构性（Heterogeneity of components）。如果要汽车的制造商来替换由不同原始设备制造商（Original Equipment Manufacturers，OEMs）所生产的所有部件，这显然是不可能的。因此，双方必须都遵守同样安全要求，安全评估和安全测试。

- 车内通信（In-car communication）。由于隔离假设，CAN网络在本质上是存在漏洞的，因此，现在需要一个假设存在潜在的恶意攻击者的新协议。

- 新的漏洞和攻击（New vulnerabilities and attacks）。在即将到来的无人驾驶车，V2V和V2I通信时代，新的安全问题肯定会出现。

结论

- 本文特别关注四个代表性的CPS应用：ICS，智能电网，医疗设备和智能车。 我们提出了威胁，漏洞，已知攻击和现有控制的分类。我们还提出了一个网络物理安全框架，并将其纳入CPS的安全方面。该框架展示了一个物理领域的攻击是如何导致网络领域中所不可预计的后果的，以及对这种攻击的解决方案。使用我们的框架，可以开发出更有效的控制手段来消除网络-物理攻击。
- 在本文中，我们还强调了CPS安全研究中的挑战和一些缺失的部分，并希望在研究界中激发更多的兴趣。

谢谢！