###
如何构建安全的系统？构建安全的系统，除了需要与安全相关的技术外，还需要考虑那些问题？
结合本课程内容，论述你的观点。
上传pdf文档
如何开发安全系统：10个设计原则 - 网络索菲亚 (cybersophia.net)
如何通过3个步骤建立可靠的网络安全战略 - 斯坦菲尔德IT (stanfieldit.com)
如何建立网络安全计划 - 网络安全战略和GRC (thepenn.group)
信息安全体系的“术”：标准主线与关联性 - 刘巍然-学酥的文章 - 知乎 https://zhuanlan.zhihu.com/p/21348250
从头开始构建网络安全战略的 7 个步骤|GRA Quantum
举例说明最好
3,4页以上

面对攻击、错误,灾难,如何保持系统可靠性

如何构建安全的系统

安全系统的需求

一、安全系统的需求

自古以来,人们一直有着对构建安全的系统的需求.在互联网高度普及的今日,系统往往与网络紧紧关联,于此同时构建安全的系统也愈发困难。

用户往往希望构建安全的系统,并且希望系统在面对攻击、错误、灾难时依旧保持可靠性.然而现实社会中存在一些威胁系统安全的因素，一旦安全系统失效，小则威胁个人隐私，大则危害到整个人类的生活与环境。

当系统面临威胁时，我们希望系统能够继续可靠地运行，而这与信息安全密不可分。

人是最大的弱点

二、系统安全威胁的类型

（一）自然威胁

自然威胁主要指的是一些自然现象，这些现象是人为不可控制和避免的，比如雷暴天气产生的电磁干扰，会影响电网信息的稳 定。尤其是一些极端恶劣天气，比如冰雹或者是台风，可能损坏电 网设备，从而威胁整个电网系统的安全。但是自然威胁比较少见， 并且影响范围有限，只是在局部地区造成了小范围的影响，产生的 损失也较小，不是智能电网信息安全威胁的主要类型。

（二）人为威胁

顾名思义，人为威胁指的是，人为故意或者是无意对智能电 网系统进行攻击，从而导致智能电网出现故障，不能正常运行，信息的安全性和保密性受到破坏，造成极大的经济损失和持久的恶劣 影响。具体而言，人为威胁还分为主动威胁和被动威胁两种。智能 电网内部操作人员错误的操作属于被动威胁，主要是使用数据的方 式和途径不正确和不规范，导致资源被误用。而一些不法分子以及 网络黑客对智能电网系统进行攻击，从而获取利益，这属于主动威 胁，而且这种威胁极为常见，同时种类多样，不一而足。下面具体 举一些这方面的的例子，帮大家简要梳理一下。第一种，不法分子 在未经授权的情况下，擅自修改系统的程序，并且控制系统的运 行；第二种，不法分子通过发送控制指令，迫使系统暂停运行；第 三种，对于计算机以及网络中的信息和资源进行窃取和监听；第四 种，通过伪造IP地址对系统进行攻击；第五种，通过木马和病毒， 制造网络故障；第六种，干扰系统的通信，造成网络瘫痪。

（三）系统威胁

对于智能电网信息系统而言，主要受到两方面的威胁，一方 面是因为信息系统自身的设计存在问题，另一方面是因为信息系统 的应用和连接存在缺陷。目前很多智能电网计算机的操作系统都是 Windows系列，逻辑方面存在不科学的地方，经常会出现漏洞，尤 其是编写错误，需要及时更新补丁，当接入互联网后，这些漏洞和 隐患就会受到强烈的攻击，从而感染木马或者病毒，进而智能电网 系统被控制，信息遭到窃取。除了操作平台，操作人员的U盘、移动硬盘都可能感染病毒，进而破坏系统。因为智能电网信息系统主 要应用的设备是智能仪表和自动装置，这些设备的组成都需要电路 板，而相关厂家在研发和生产的过程中，设计以及制作工艺都不可 能尽善尽美，稍有不慎，就会招致数据的损失或者是泄露，进而发 挥不了应有的功能。目前，也有一些厂家故意在芯片中植入恶意程 序，之后破坏电厂的系统，导致电厂在计算电量时出现误差，造成 数额巨大的经济损失。而且智能电网信息系统经常需要在不同设备 和网络之间进行连接，那么具体的数据通信就要遵守和执行TCP/IP 协议，但是因为协议明文传送，所以很容易被获取，之后不法分子 就可以伪造数据，传输错误和虚假的信息。

【【智能电网信息安全威胁及防御技术研究】】

相关安全防御技术

一、安全框架四要素

- 策略(Policy):指明要达到的目标。
- 机制(Mechanism) 为了实现目标所采用的运行方式
- 保证(Assurance):每种特定机制的可靠程度
- 动机(Incentive)系统保护、维护人员正确履行职责的动力

二、技术层面上信息安全的相关防御技术

所谓信息安全就是要保证信息的保密性、完整 性、可用性和不可否认性。信息安全防御技术主要 包括加密／解密技术、身份认证／数字签名技术、入侵 检测和防御技术、基于角色访问控制技术、防火墙技 术、安全隔离技术和虚拟专用网络（ＶＰＮ）等。在保 障信息安全各种功能／特性的诸多技术中，加密技术 和身份认证技术是信息安全防御技术的核心和关 键。加密技术是最基本、最常用且最有效的信息安 全防御技术，可以有效限制非法侦听、截获、中断、伪 造的概率，从而达到保证报文／信息安全的目的。入 侵检测技术是满足机密性、完整性、可用性安全需求 的关键技术之一。防火墙是一种安装在组织机构的 内部网络与互联网之间的设备，是保证网络层安全 的边界安全工具。安全隔离装置（网闸）是一种网络 安全设备，它包含带有多种控制功能的专用硬件，可 在电路上切断网络之间的链路层连接，并能在网络间进行安全适度的 应 用 数 据 交 换。ＶＰＮ 为网 络 间 传送数据和控制信息提供了一种安全的通信机制， 它在隧道模式下使用ＩＰＳｅｃ来提供保密性、完整性、 数据源鉴别、重放保护和访问控制的数据保护

（一）信息加密技术

这种技术应用的基础是特殊算法，从而对数据进行加密处理， 当数据传达之后再进行解密和还原。即使不法分子拦截和获取了加 密信息，因为不了解和没有掌握解密的具体方法，所以无法知晓和 得到原始的信息，这就切断了信息之间的联系，防止数据被利用。 将重要信息进行伪装，也就是进行数学变换，将明文变成密文， 需要注意的是，这种加密是双向可逆的，所以智能电网信息系统可 以对信息进行加密，从而提高系统的稳定性。比如使用对称加密算法，也就是使用同一种密钥进行信息的加密和解密，只有信息的接收者和传输者都掌握一致的密钥，才能解密信息。另外，密码的设 置也是极为关键的，很多不法分子在面对复杂的密码时，常常因为 破解耗时耗力，成本巨大，就直接放弃，这在很大程度上保证了 信息的安全。密码一般由数字、符号以及字母组成，长度在8位以 上，并且需要定时更换

（二）签名认证技术

通过电子签名，能够识别数据的真实性和可靠性，而且电子签 名与手写签名的作用相等。这种签名认证技术，主要是对数据单元 添入密码，杜绝伪造现象，从而保证数据的接收方准确获得完整的 数据。智能电网通过在信息终端部署统一的数字证书，能够很好地 对参数以及计费等信息进行认证，同时可以实现信息的遥控

（三）漏洞隔离技术

对于系统存在的漏洞，需要应用隔离技术，常用的做法是安 装防火墙。防火墙的信任等级很高，能够很好地保证信息服务的质 量。也就是说防火墙是一道有效的屏障，通过在智能电网以及互联 网之间设置防火墙，能够筛选网络中的信息，外部用户如果想要访 问智能电网，就需要经过防火墙，这就为智能电网营造了一个良好 的内部环境，排除了外界不良信息的干扰。

（四）病毒查杀技术

目前，计算机病毒的数量与日俱增，同时种类异常丰富，能 够不同程度地攻击计算机系统，严重威胁着信息的安全。通过使用 专门的程序，对病毒进行查杀，能够对信息进行检测，确定病毒的 存在或者是病毒的感染，之后根据查杀情况，对信息进行相应的处 理。一般而言，安装防病毒程序并不会影响系统的运行速度，而且 针对性很强，能够及时发现病毒，并且彻底清除。

（五）入侵检测技术

智能电网信息系统需要做好入侵监测工作，对任何未经授权 和可疑的行为进行拦截。整体而言，入侵监测分为三方面：第一方 面，对信息进行搜集，也就是要全面监测网络以及用户的行为，保 证信息的准确。第二方面，对数据进行分析，根据已有模型进行匹 配，从而做好统计分析工作。第三方面，对结果进行响应，一般而 言，如果对入侵行为进行阻止和控制，就是积极响应，如果只是发 出警报，就是消极响应。

（六）蜜罐诱捕技术

如果想要保证服务器不受黑客等不法分子的攻击，可以在网络 中添加蜜罐子网，这样能够形成一个诱捕机制，进而引诱黑客对蜜 罐进行攻击。这样能够减轻服务器的压力，并且完整地记录黑客的 行为，智能电网信息系统可以适当应用这种技术，将黑客的恶意攻 击进行分流，从而保护系统的安全。

三、安全技术之外的防御技术

安全系统的构建

一、信息安全防御体系的构建

不同类型安全系统，既有共性又各有特性，其构建方式也略有不同。

（一）以乌克兰和以色列国家电网遭受网络攻击事件为例

1. 背景知识

智能电网是一种典型的信息物理融合系统，由 传统电力基础架构与信息基础架构共同组成。智能电网的安全问题包括物理安全和信息安全两个方 面。智能电网信息化及其物理系统与信息系统的深 度融合为其引入了新的安全隐患，针对信息系统的 网络攻击在破坏其功能的同时，也会传导至物理系 统并威胁其安全运行。近几年来，通过网络攻击智 能电网并进行破坏的事件时有发生。

２０１５年１２月２３日，乌克兰电网遭遇突发停电事故，引起乌克兰西部地区约７０万户居民家中停电 数小时。事后研究人 员 表 示，这 是 由 BlackEnergy（黑暗 力 量） 恶意 软 件/代 码 导 致 的 破 坏 性 事 件。在此次攻击事件 中，运用了其最新版本 BlackEnergyLite，并增添了 KillDisk 组 件 和 SSH安 全 外 壳 协 议 ）后 门。KillDisk 组件用于删除计算机硬盘驱动器里的数据 并导致系统无法重启。SSH 后门在获得 SSH 服务 器的访问权限后，开放连接 SSH 服务 器 的6789端 口，从而使攻击者可以永久访问或控制受感染的 SSH 服务器。该停电事故被视为实际出现的首例针对供电系统的恶意行为。

２０１６ 年 １月２５日，以色列电力局遭受了一次严重的网络攻击。在此次攻击事件中攻击者 发送包含勒索软件（Ｒａｎｓｏｍｗａｒｅ）的钓鱼邮 件给 电 力局工作人员，诱骗电力局工作人员执行恶意代码， 并加密其电脑中的相关内容，需要电力局工作人员 付款才能解锁。事发后，以色列当局被迫关闭了电 力设施中被感染的计算机，以防止勒索软件在网络 中进一步传播，引发更大的事故。

由乌克兰和以色列国家电网遭受网络攻击事件 可以得到如下启示。

１）电力系统作为国家关键性基础设施已经成为 网络攻击的重要目标，网络攻击能达到类似于物理攻击的效果，从而导致变电站乃至整个能源供给系 统的瘫痪。

２）攻击者具备一定的电力系统工程背景，对变 电站监控系统软件及电网业务流程都非常了解，其 发动的针对电力系统的攻击具有很高的技术含量。

3）工业界还没有为此类网络攻击做好准备，电 力系统中信息基础设施的脆弱性客观存在，面对网 络攻击时表现得非常敏感，现有的信息安全防御体 系难以完全有效抵御此类网络攻击。

美国国防 部 高 级 研 究 计 划 局（ＤＡＲＰＡ）近期 启动了一项名为“快速攻击检测、隔离和表征”的计 划，目标是发展一套能够应对电网遭受针对信息网 络或基础设施 的 摧 毁 性 攻 击 后，７ｄ内恢 复 电 力 供应的自动化系统。针对电网的网络攻击很可能是出 于政治、军事或者经济的目的，可以说，智能电网的 信息安全防御已被提升为一个国家安全层面的重要 问题。

依照目前的国际形势，包 括欧美国家在内的其他国家，与中国发生正面战争的机会微乎其微。然而，发动黑客、罪犯和恐怖分子 通过通信网络对中国的重要基础设施（如核电站、三 峡水电站和国家电网等）进行破坏，从而阻止或延缓 中国经济发展的可能性很大。

2. 人

人是信息系统中最不稳定、最不确定，也是最危险的因素；特别是内部人员，是信息安全的最大威胁。因此，需加强 管理、制定完善的信息安全制度。

3. 底层通信节点

加强对系统智能核心物理组件的监测和管理。系统中的一些物理设备在 实现测量、保护、监控、通信等功能的同时，其本身作为底层通信节点，是系统通信网络的主要组成 部分之一。黑 客 很 有 可 能 入 侵 并 潜 伏 在 这 些物理设备中，在满足一定的触发条件时才开始执行 恶意程序。这类攻击具有很深的隐蔽性，采用通用 的入侵检测技术很难发现。黑客对这些设备的攻击效果一定会体现在某些物理特征上，可以通过发现 这些设备在时间、空间和控制指令执行效果等方面 的异常表现来检测这类攻击。

4. 物理隔离

电力系统各个单位办公系统／网络与电力监 控系统／网络进行物理隔离，禁止 U 盘和移 动 硬 盘 等存储介质在两个系统／网络之间交叉使用，禁止在电力监控计算机中打开办公文档或电子邮件。攻击 乌克兰和以色列国家电网的病毒软件即是通过电子 邮件传播。

5. 协同各单位采用统一的信息安全防御策略，

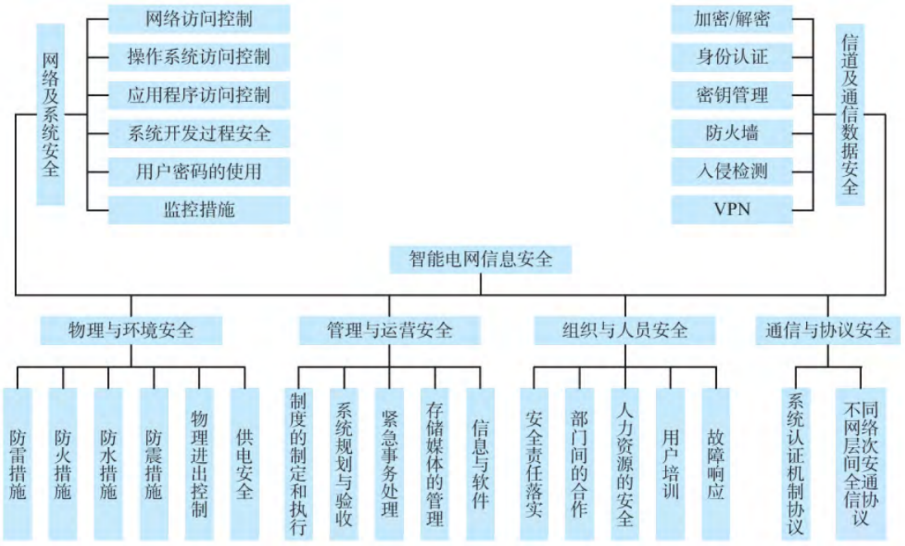
构建一体化信息安全防御体系。电力系统主要包括 发电、输电、变电、配电、用电和调度 6 个环节，涵盖 运行、管理、控制和市场等方方面面，各环节的信息 安全体现出不同的需求。整个电力系统的信息安全 水平遵从“木桶原理”，哪个环节或组成部分的信息 安全防御水平最低，该环节或组成部分

即成为电力 系统信息安全防御最薄弱、最易攻破之处。因此，需 要协同各单位进行统一部署。

6. 加 密 / 解密算法和身份认 证 / 数字签名算法

（二）体系构建

从严格意义上讲，不存在绝对安全的网络，系统 的安全和开放本身就是互相矛盾的。因此，需基于 “适度安全”和“尽可能透明”的策略，明确智能电网 的信息安全需求和为实现信息安全保障要求所增加 的投入，在保证信息传输的可靠性、实时性前提下制定智能电网信息安全策略，定义信息的共享方式和 安全级别，寻找信息安全和共享（开放）、信息传输实 时性与系统安全性之间的平衡点，提出信息安全最 佳实施方案。



*智能电网信息安全防御体系与...受网络攻击事件的思考与启示_李中伟.pdf

（三） “适度安全”和“尽可能透明”的策略

“适度安全”和“尽可能透明”的策略，例如限制密码猜解次数其显然有着抗穷举攻击的优势，但对于普通用户而言，又有着被拒绝服务的风险，反而会给用户带来不便。

系统安全的绩效依赖的是最弱环节

二、安全相关技术之外

（一）关于定义

很多系统宣称自己安全因为硬件而被认证为安全可能超出预期忽略人为因素忽略可用性

缺乏明确性:证明了什么?

定义模糊身份与名字 人与自然人 信任与可信任 保密、隐私、机密性

保密:限制可以访问信息的主体数量的机制的效果

机密性:为别人保守秘密的职责

隐私:保护个人信息的能力和权力,防止别人侵入个人空间。(家庭,不包括公司法人)

保护对象是谁？第一步应该对系统有着明确的定义，如银行系统的安全定义与医疗系统可能有很大的不同

（二）基于心理学的攻击与防御

电影《我是谁：没有绝对安全的系统》中将社会工程学看作伟大的欺骗艺术，其中提到“人究其本性极易受骗，也怕冲突”，利用人这两点特性可以攻破许多系统。系统常常不是被从系统安全层面上攻破，而是人。

正如同攻击者获取一般用户银行卡密码或支付密码的最有效方式是通过摄像头等偷看一样，无论系统设计的多么完备，攻击者依然可以绕过系统的防御，系统坚固的防御此时如同法国所修建的马奇诺防线一样在此时变得毫无用处。

生物识别的活体检测必要。

系统最好能够对入侵者起到威慑作用。

参考文献