- IEC62443-1-1
  - 范围
  - 术语和缩略语
  - 规范性引用文件
  - 概念
    - 信息安全目标
      - 保密性
      - 完整性
      - 可用性
      - 某些情况下，重要程度可用性>完整性>保密性
    - 基础要求
      - 使用控制
      - 数据完整性
      - 访问控制
      - 限制数据流
      - 事件及时响应
      - 资源可用性
    - 纵深防御
      - 分层城市防的多重防御
    - 信息安全上下文
      - 信息安全各个要素之间的相互关系
        -
        - Floating Topic
    - 威胁-风险评估
      - 资产
        - 分类
          - 人员资产
          - 物理资产
          - 逻辑资产
        - 价值评估
          - 定性/定量
          - 直接/间接
      - 脆弱性
        - 随环境，技术，组织目标，变化，人员活动，更高级威胁的出现而变得更加脆弱安全态
      - 风险
        - 基本评估过程
          - 风险初期评估
          - 实施风险缓解对抗措施
          - 评估剩余风险
          - 常需要重复进行
        - 典型风险
          - 人员安全
          - 过程安全
          - 信息安全
          - 环境风险
          - 业务连续性风险
        - 风险容忍等级
          - 不同组织容忍度不同
        - 风险响应
          - 设计排除风险
          - 降低风险
          - 接受风险
          - 转移/分担风险
          - 排除/重新设计冗余/无效的控制
      - 威胁
        - 常见形式
          - 偶然事故
          - 未经确认的修改
        - 威胁代理
          - 内部人员
          - 外部人员
          - 自然灾害
        - 被动威胁
          - 信息泄露
        - 主动威胁
          - 篡改
          - 数据库注入
          - 重放
          - 欺骗与假冒
          - 社会工程
          - 网络钓鱼
          - 恶意代码
          - 拒绝服务
          - 权限提升
          - 物理破坏
        - 对抗措施
          - 用户/计算机鉴别
          - 访问控制
          - 入侵检测
          - 加密
          - 数字签名
          - 资源隔离与分离
          - 恶意软件扫描
          - 系统活动监视
          - 物理安全
    - 安全程序成熟度
      - 阶段
        - 概念
          - 识别
          - 概念
        - 功能分析
          - 定义
        - 实施
          - 功能设计
          - 详细设计
          - 建设
        - 运行
          - 运行
          - 符合性监视
        - 回收和处置
          - 处置
          - 拆解
    - 策略
      - 目标
        - 导则
        - 规程
        - 策略
      - 涵盖主题
    - 安全区域
      - 区域内的区域
        - 隔离分层安全性
      - 边界
      - 分类
        - 被信任/不被信任
        - 物理划分/逻辑划分
    - 管道
      - 管道是一类特殊的安全区域
      - 通道
        - 可信
        - 不可信
    - 信息安全等级
      - SL目标
        - 应该实现的效果
      - SL能力
        - 固有安全属性
      - SL达到的
        - SL能力
        - 建立通信的区域的SL达到的
        - 管道相关安全属性
        - 对抗措施效果
        - 审计和测试间隔
        - 攻击者可用的知识和资源
        - 固有安全属性的降级
        - 入侵检测
        - 顾问
    - 信息安全等级生命周期
      - 评估
      - 开发和实施
      - 维护
  - 模型
    - 参考模型
      - 4级 | 企业系统
      - 3级 | 运营管理
      - 2级 | 监督控制
      - 1级 | 本地/基础控制
      - 0级 | 过程
    - 资产模型
      - 地理位置
        - 控制中心
        - 远程站
        - 区域
        - 流水线，工段，它们，车辆
        - 监督控制设备
        - 控制设备
        - 现场I/O网络
        - 传感器和执行器
        - 安控设备
    - 参考体系结构
      - 资产模型中定义的实体组成
    - 区域和管道模型
      - 区域的属性
        - 信息安全策略
        - 资产清单
        - 访问要求和控制
        - 威胁和脆弱性
        - 信息安全选择后果
        - 授权的技术
        - 改变管理的过程
      - 管道的属性
        - 所有区域的属性
        - 联通的区域
    - 模型间的关系
      - IEC62443-2-1

Trial Version XMind:ZEN Trial Version