RSA CONFERENCE CHINA 2011
2011 信息安全国际论坛

the adventures of alic e & bob

新计算环境下的风险管理反思

潘柱廷
启明星辰公司 首席战略官
中国计算机学会 理事

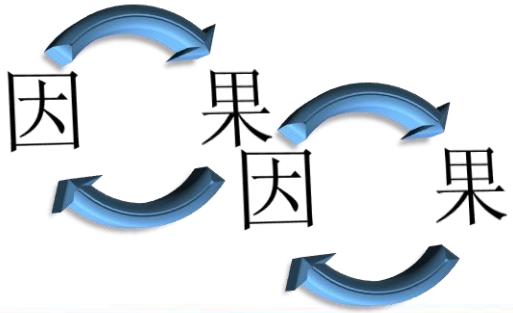
摘要

观瞰

- 风险管理方法
- 传统信息安全风险管理
- 新计算环境
- 风险管理的困惑

反思

- 风险管理的根本是什么？
- 新计算环境到底带来哪些根本变化？哪些没有变化？
- 新计算环境对于风险管理带来哪些变化需求？
- 风险管理怎么向前进步？



回顾#风险管理#

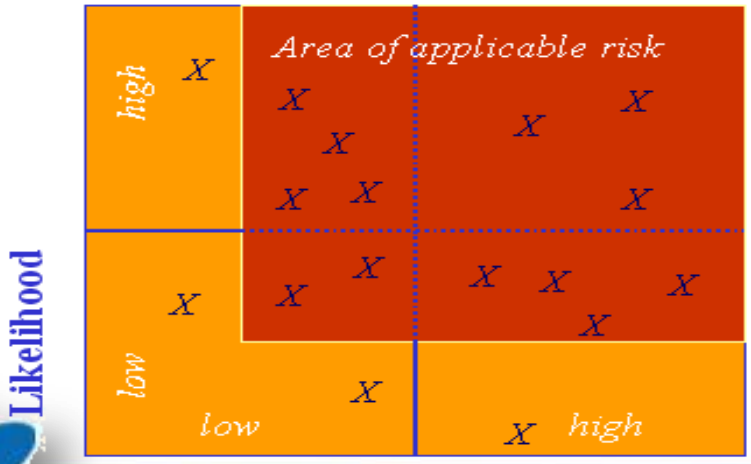
非特定领域风险管理思想

风险的概念

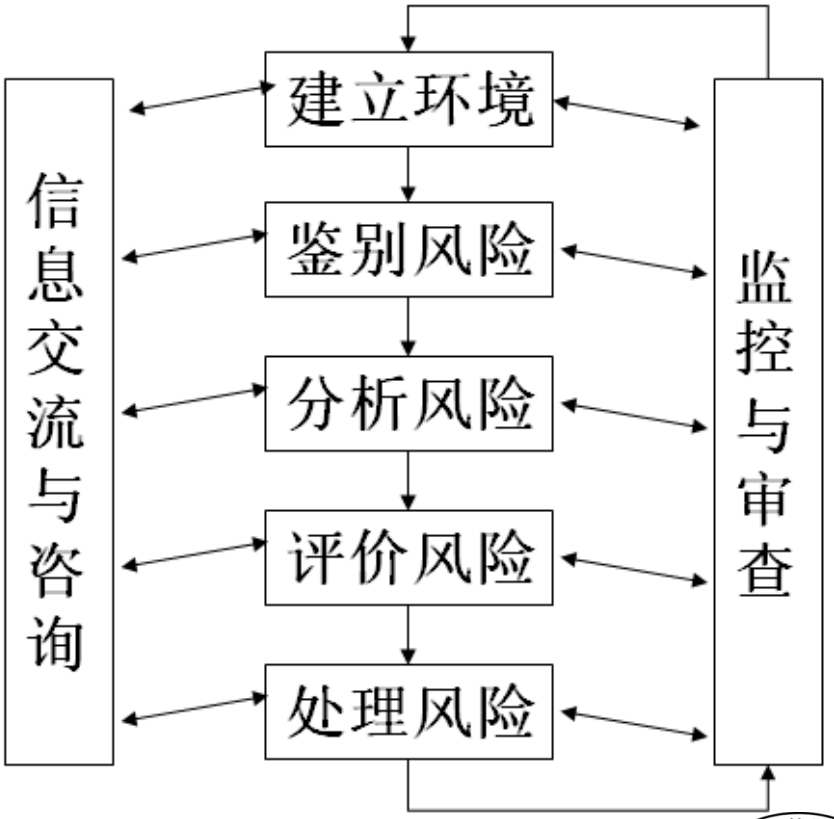
- 风险：

  对目标有所影响的某个事情发生的可能性。它根据后果和可能性来度量。

  -AS/NZS 4360:1999《风险管理》



风险管理的方法



信息安全领域的典型风险观—要素

- 风险：指定的威胁利用单一或一群资产的脆弱点造成资产的损失或损坏的潜在的可能性。

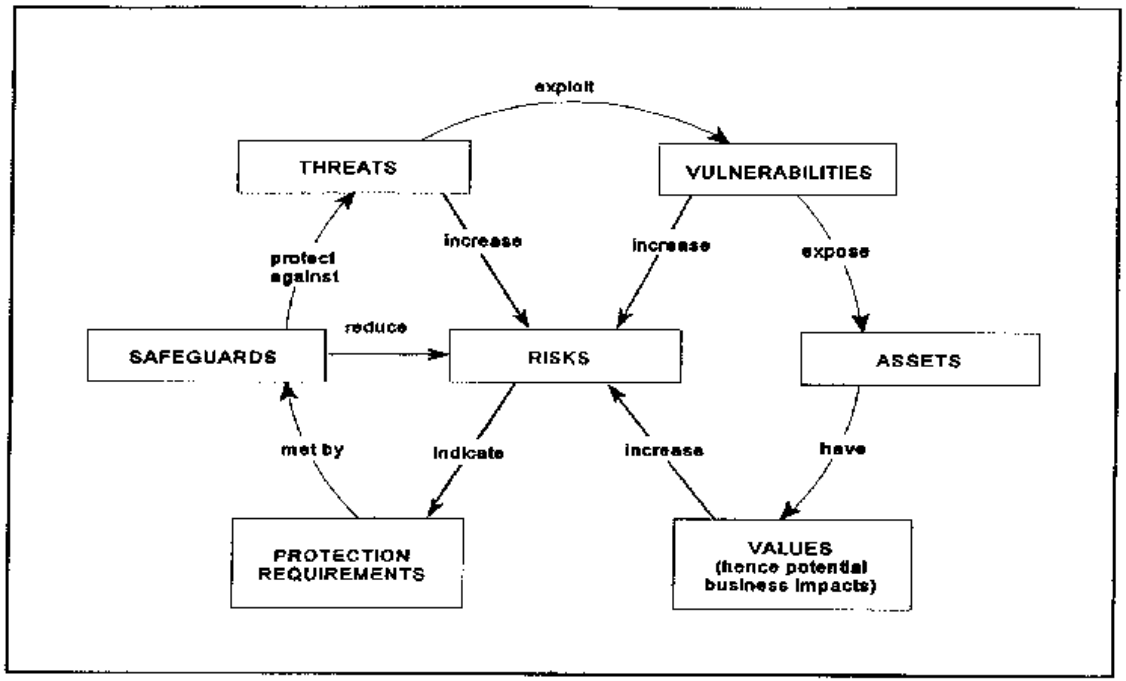
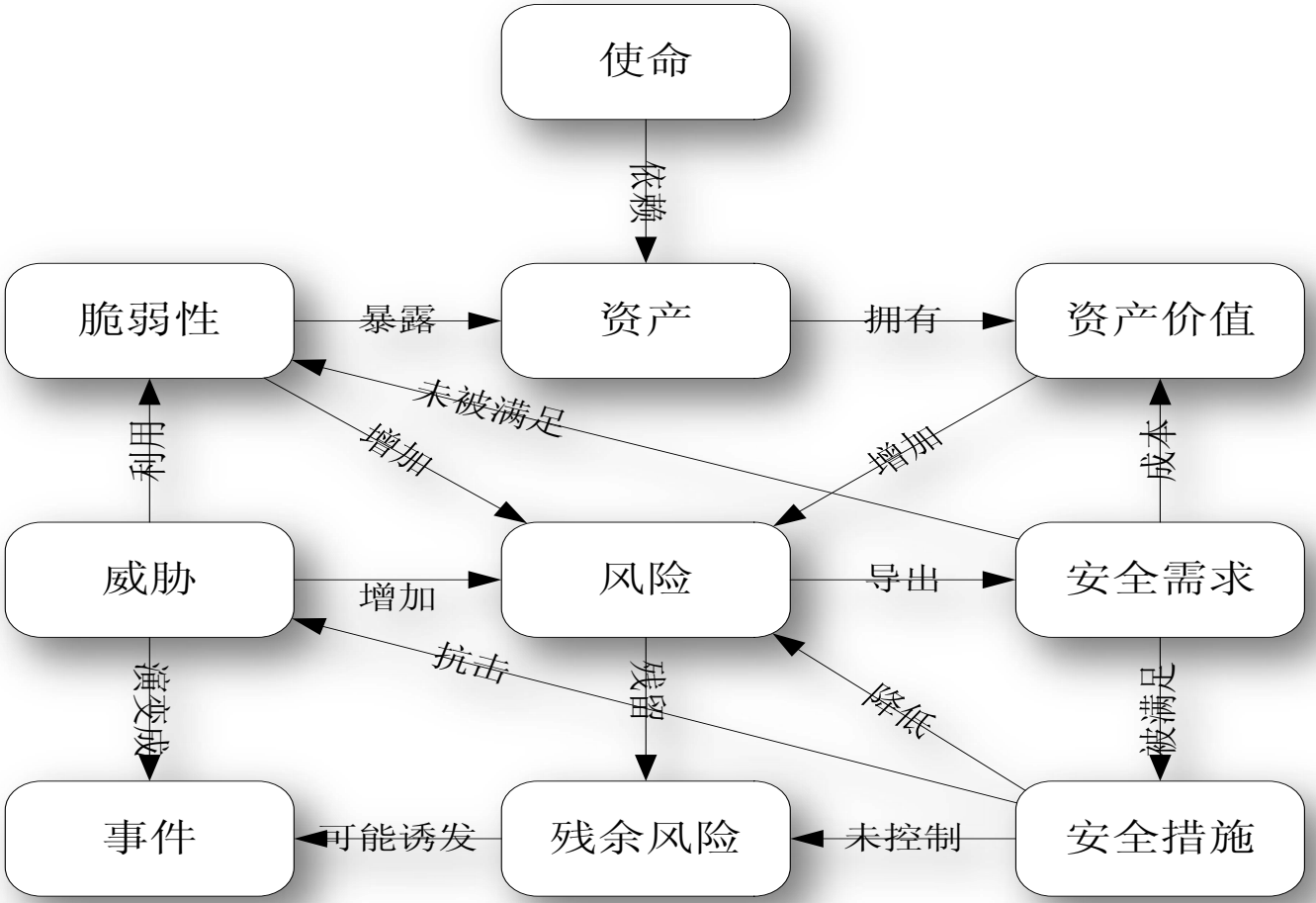


Figure 4: Relationships in Risk Management

风险评估国标中的10要素示意图



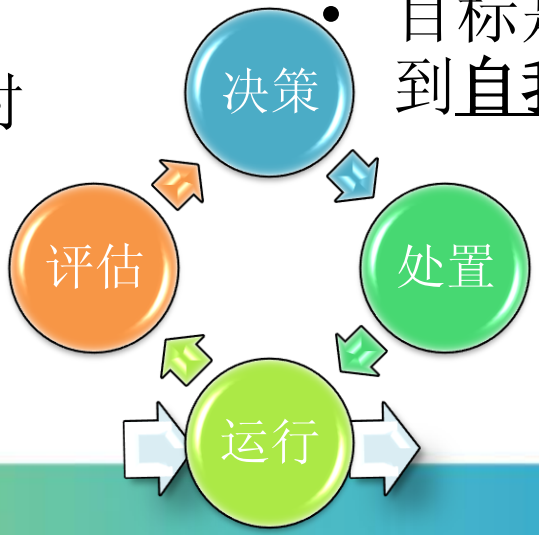
风险管理的基本目的

评估

- 最后落在评估和评价环节
- 评价的对象可以是
  - 系统状态、事件、措施、风险值
- 获得的是评估的量化或定性的结论
- 常用于**合规性**比对

处置

- 最后落在问题和事件的处置环节
- 主要行为是
  - 漏洞的修补、攻击的阻断和反击、危害的消除
- 目标是：问题的解决，达到**自我认为的安全状态**

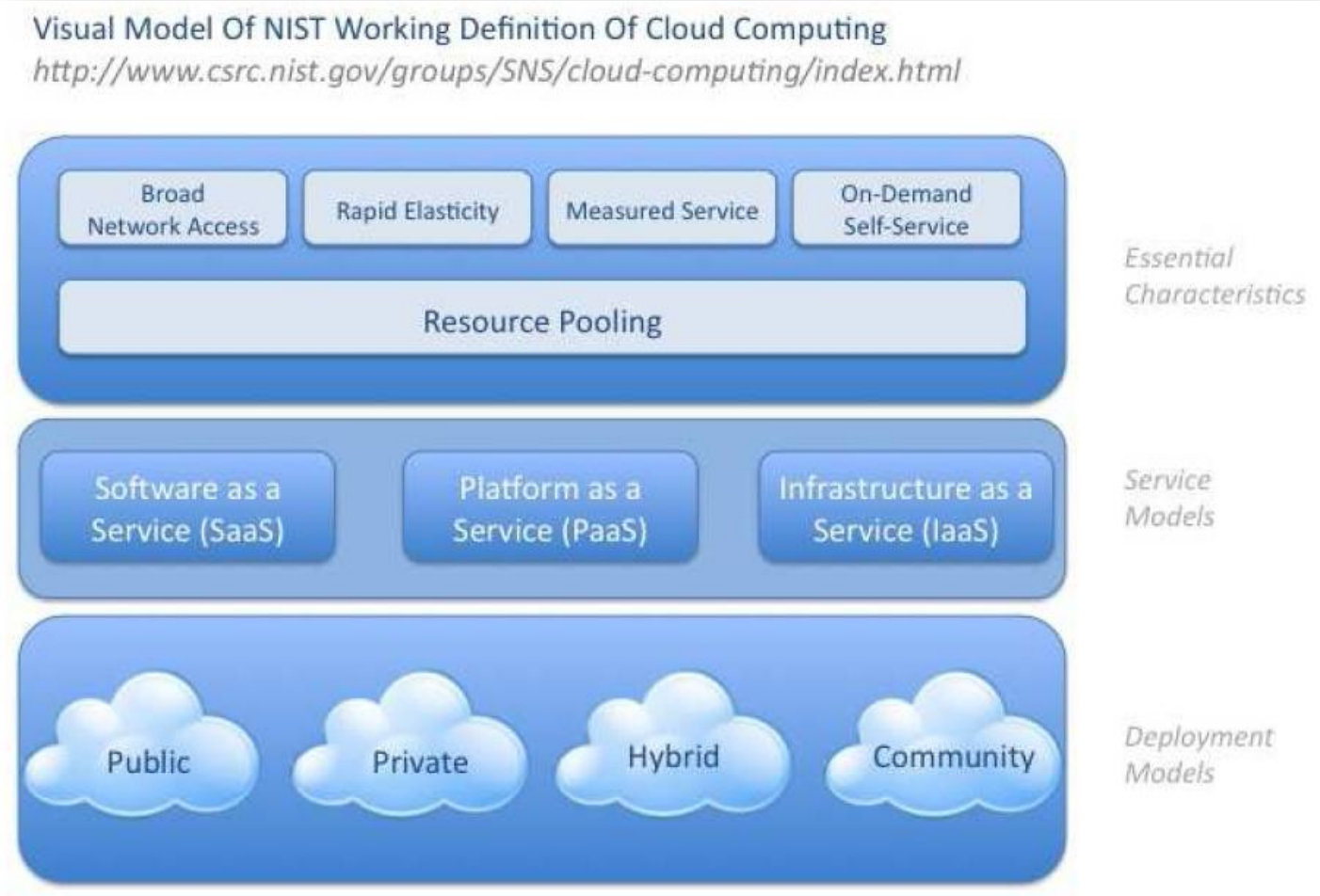


所谓新计算和新计算环境

——原有的流(过程)被颠覆

新计算到底带来了哪些变化

关于#云计算#



NIST给云计算定义了五个关键特征、三个服务模型、四个部署模型。

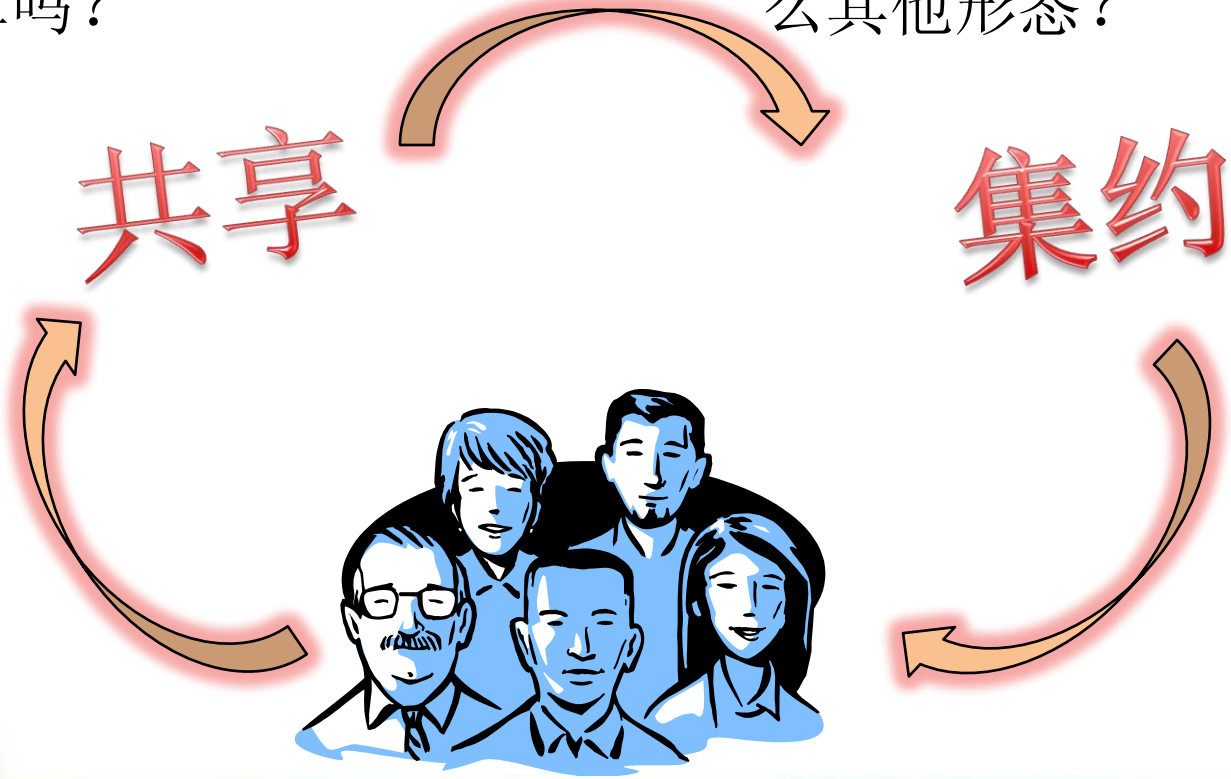
云 ？虚拟化、数据中心

虚拟化

- 如果没有虚拟化，还有云计算吗？

数据中心

- 除了数据中心，云还有什么其他形态？



关于#云计算和虚拟化#

云计算

- 原先完全在自我控制下的区域和业务流，有相当的部分不在直接掌控下了
- 虚拟+集约后，价值系统的位置都不清晰了
- 干系主体者复杂化了，至少多了租户环节

虚拟化

- 原先习惯的安全域及其边界找不到了（并不是不存在了）

关于#移动计算#

移动计算本身的特性

- 终端的变化
- 组网的变化
- 业务的变化
- 用户的变化

移动计算带来的安全问题

- 更容易产生针对具体个体的攻击
- 无线网络带来的新问题（单跳）
- 新的设备和操作系统平台所引入的问题

关于#物联网#

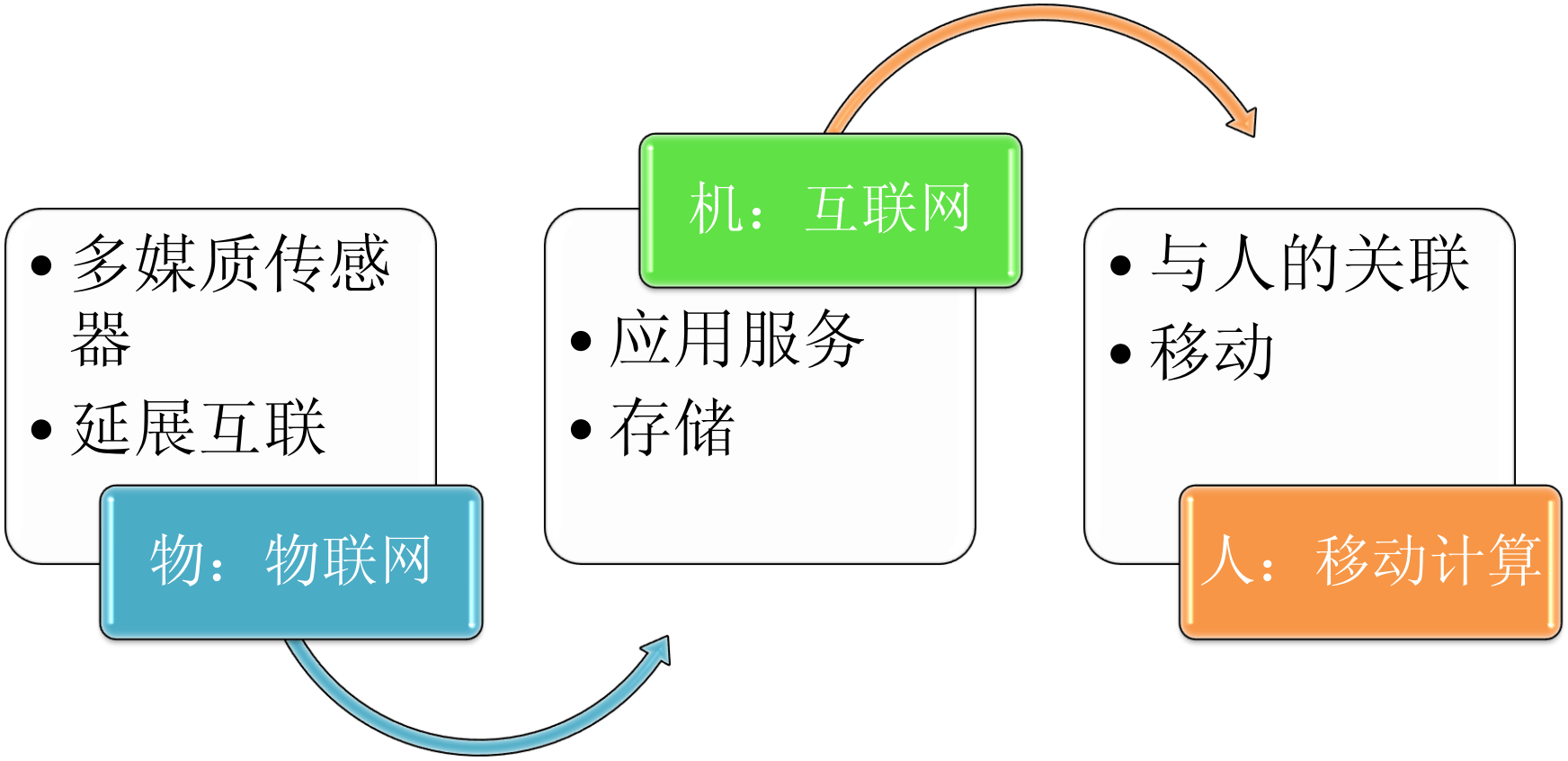
物联网本身的特性

- 多媒质的前端
- 组网方式的多样性
  - RFID
  - 无线传感网
  - AdHoc
  - DTN
- 超海量的数据处理

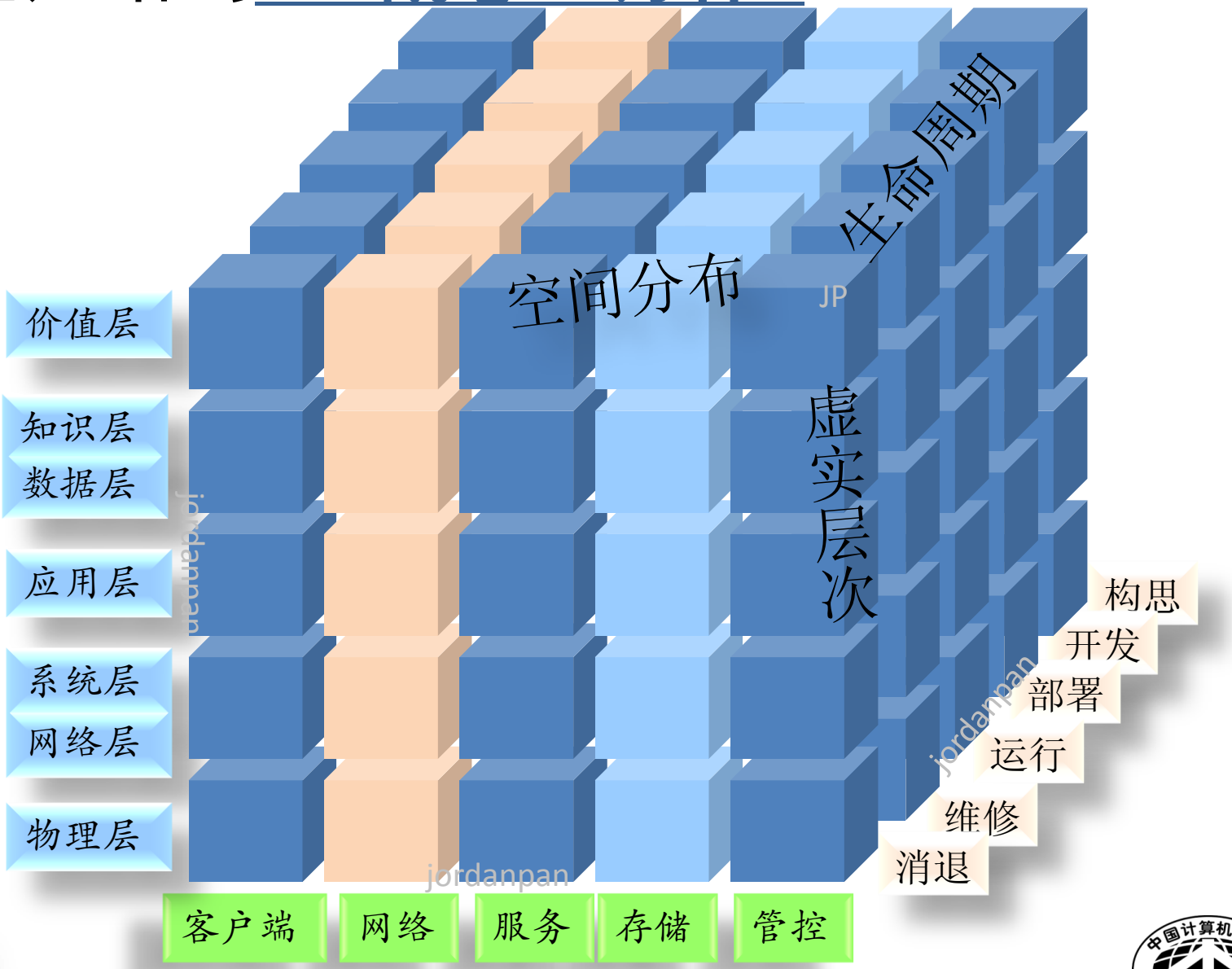
物联网带来的安全问题

- 原先不上网的”东西”都上网了。
- SCADA系统等基础设施也不可避免地上网了
- 应用的方便同时也带来攻击的方便

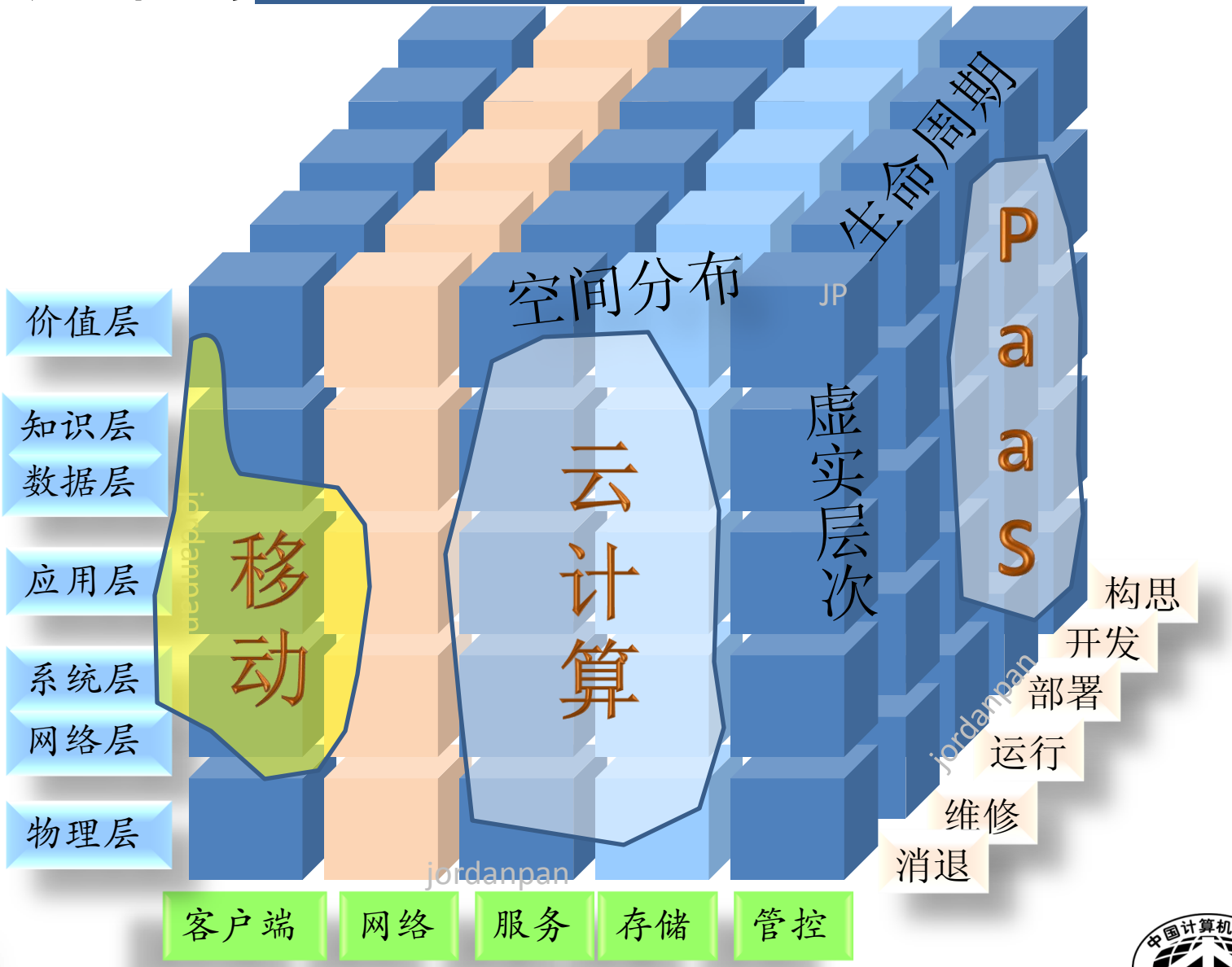
人-机-物的体系



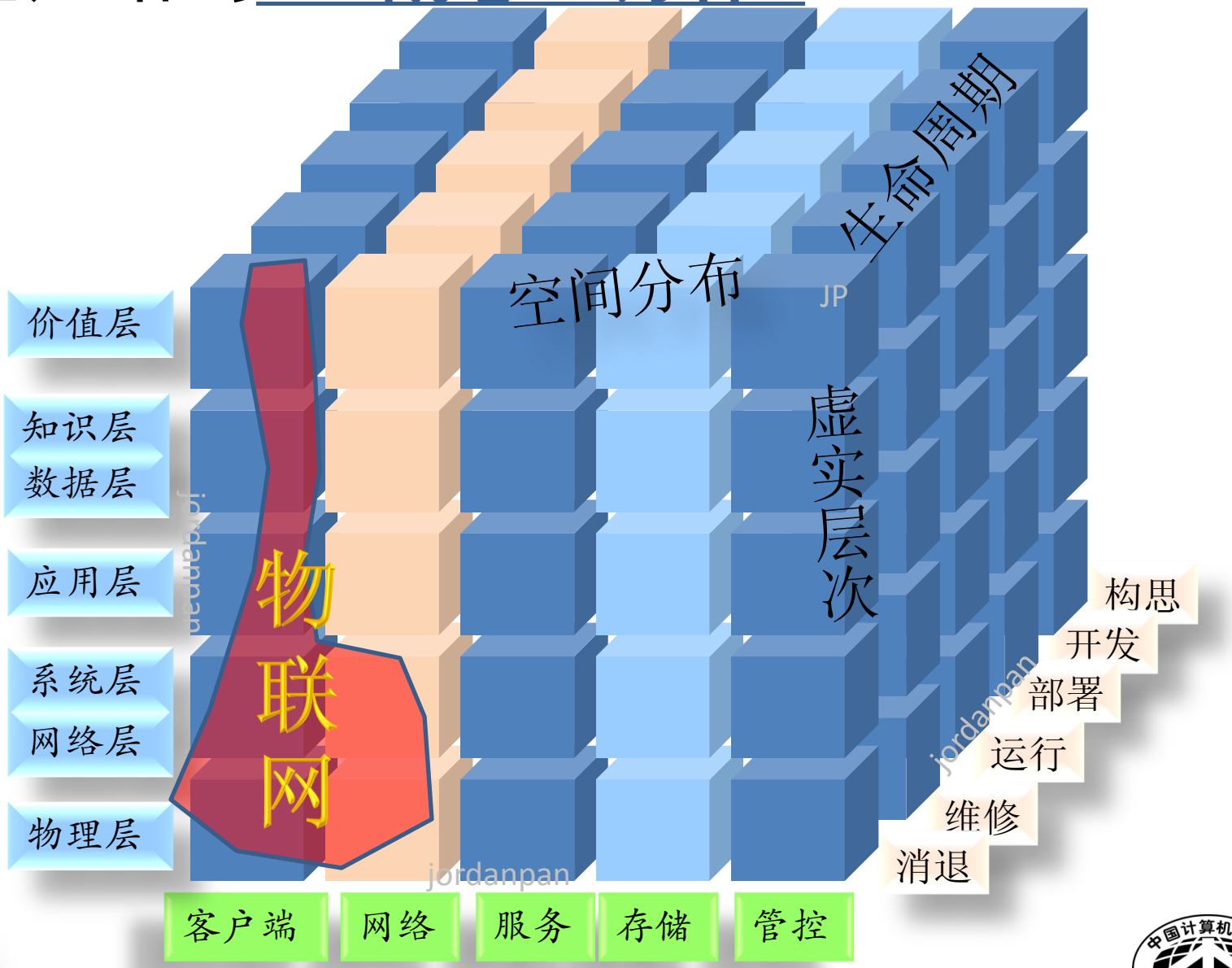
还是归结到#IT概念立方体#



还是归结到#IT概念立方体#



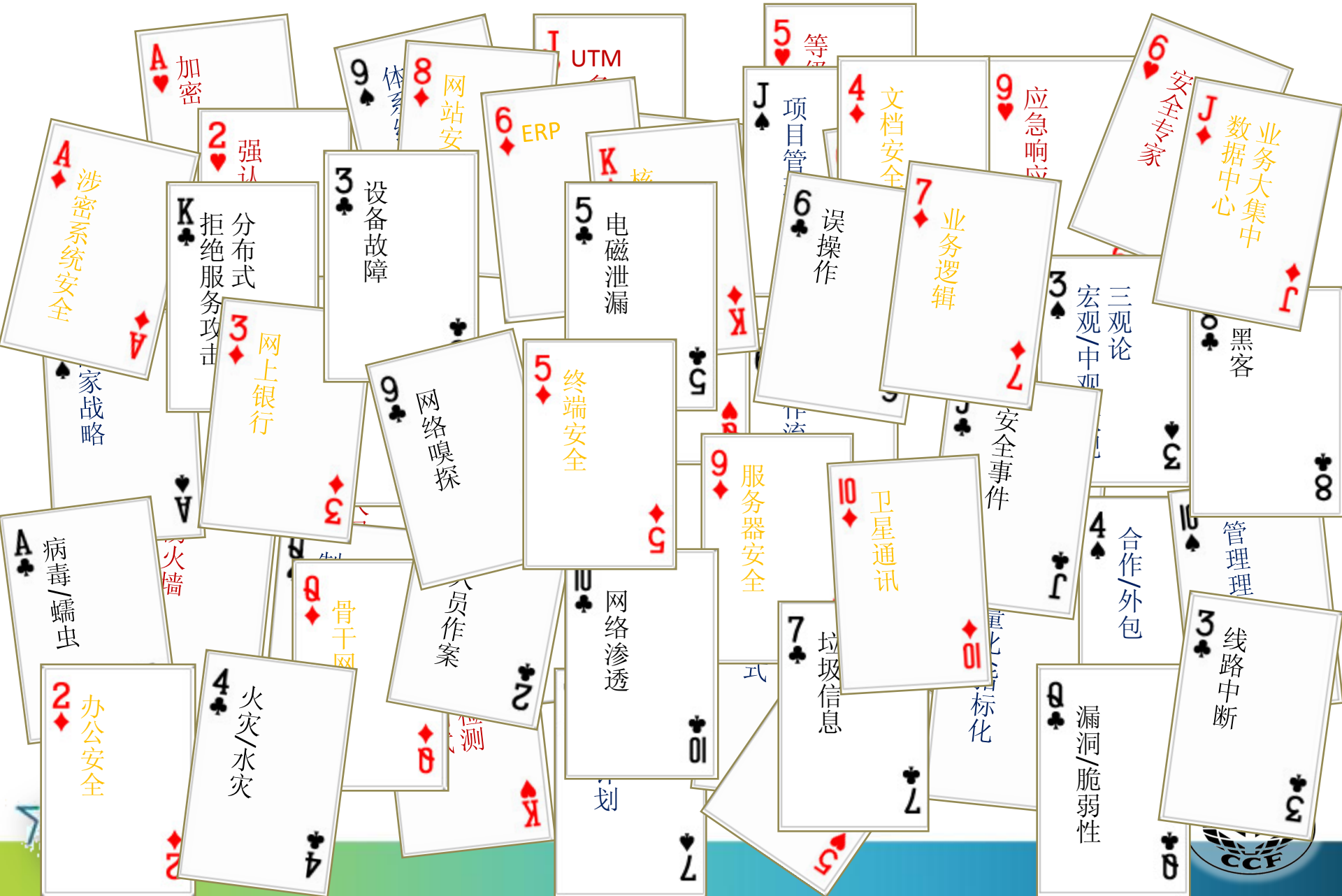
还是归结到#IT概念立方体#



IT概念立方体：空间-时间-逻辑三维 by jordanpan

#风险三要素#观念统摄风险管理
——流观(过程观)

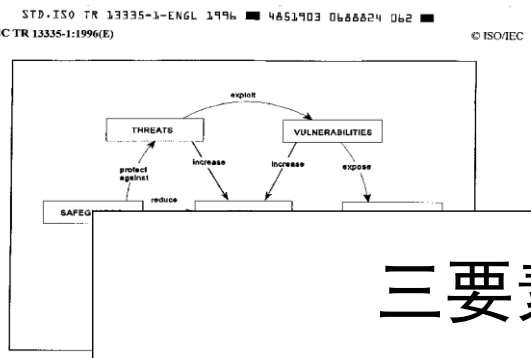
谈安全方案涉及到的方方面面

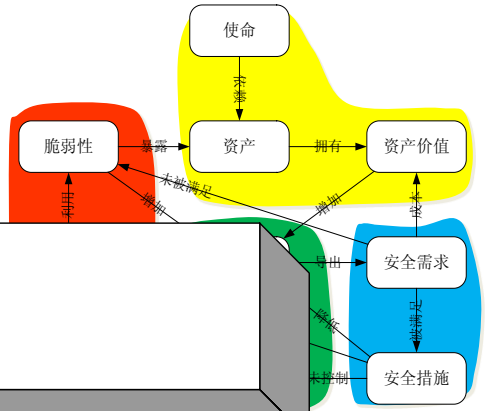


梳理手上的牌


涉密系统
办公安全
网上
骨干
网站安全
ERP
服务器
核心业务
终端安全
文档安全
业务逻辑
卫星通讯
业务大集中
数据中心
病毒/蠕虫
拒绝服务攻击
火灾/水灾
设备故障
内部人员作案
网络渗透
电磁泄漏
误操作
垃圾信
安全事件
漏洞
线路中断
加密
强认证
防火墙
入侵检测
攻击检测
渗透测试
UTM
多功能网关
审计
管理平台
风险评估
等级保护
监控/预
冗余/备份
应急响
值班安全官
安全专家
国家战略
组织体系
制度/规则
工作流
体系结构
规划/计划
云模式
项目管理
合规性
三观论
宏观/中观/微观
量化/指标化
合作/外包
管理理念

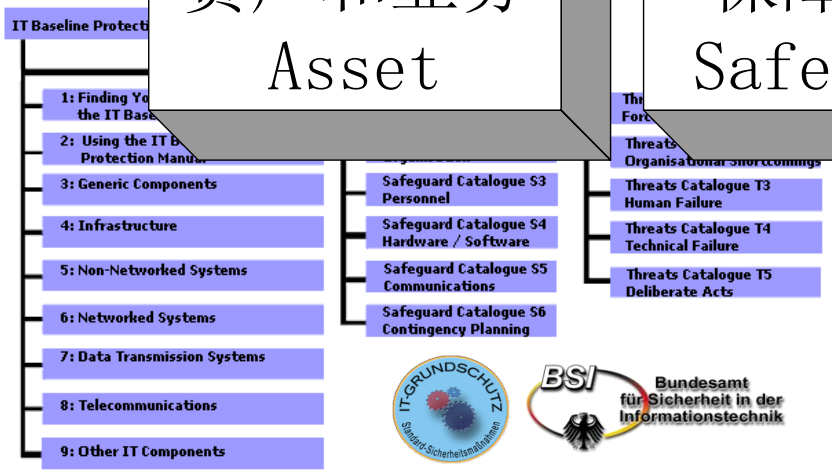
风险三要素

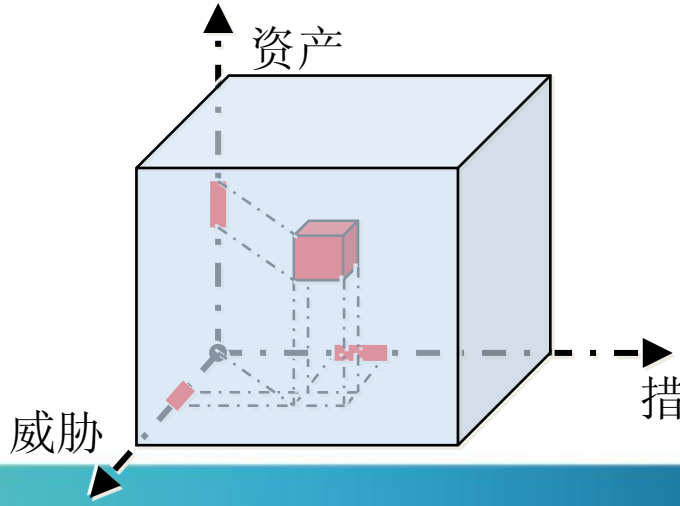




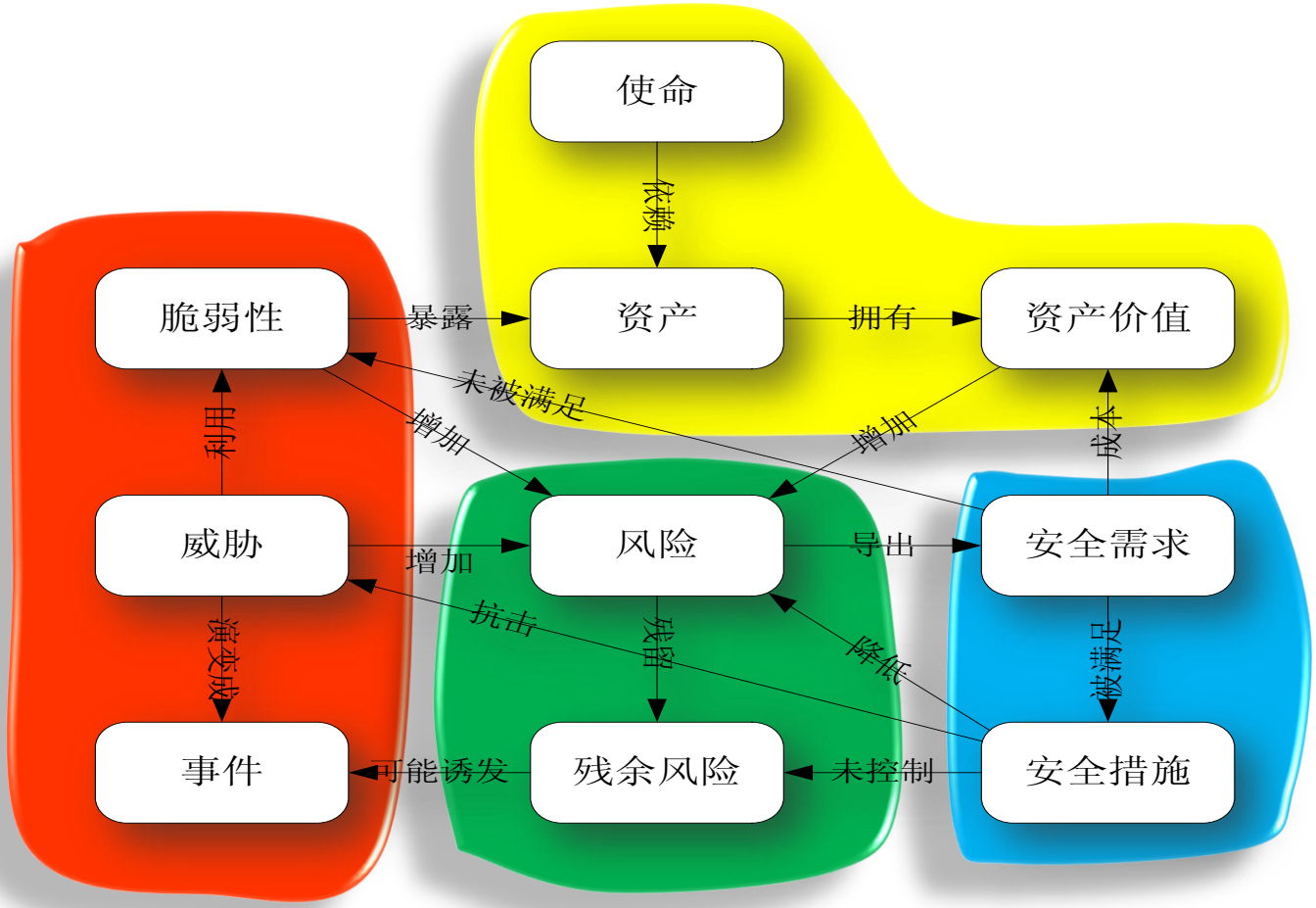
三要素风险模型：R3-AST

资产和业务 Asset	保障措施 Safeguard	威胁 Threat





风险10要素与三要素的对应示意图



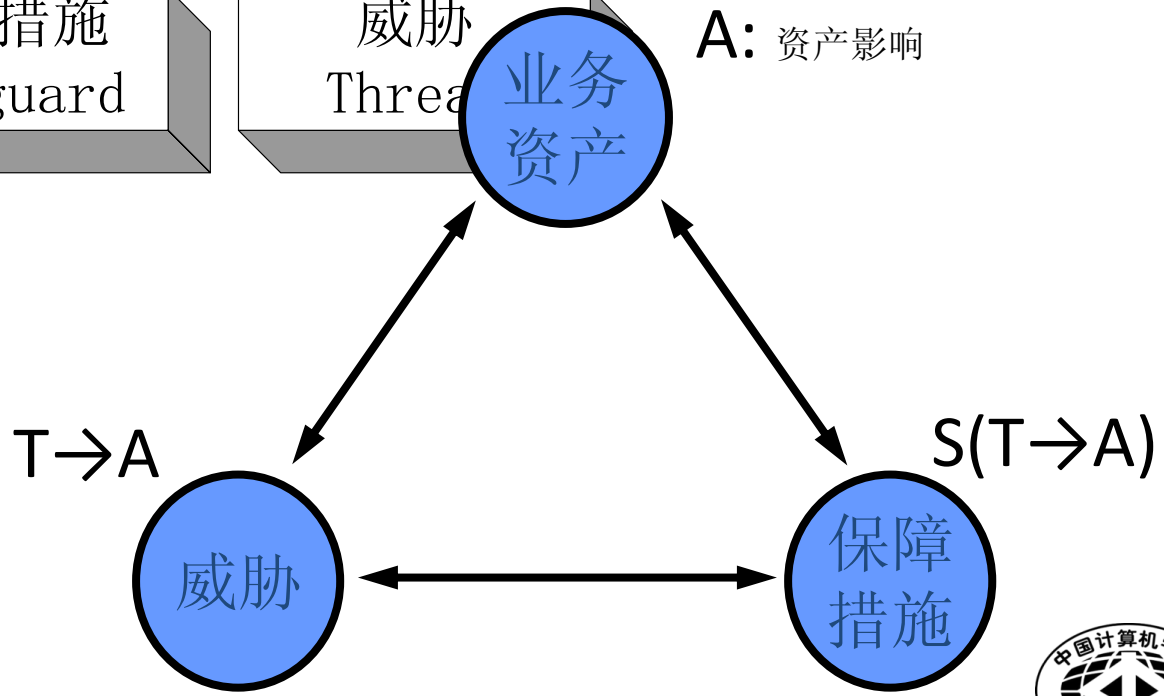
最精简的风险管理三要素

三要素风险模型：**R3-AST**

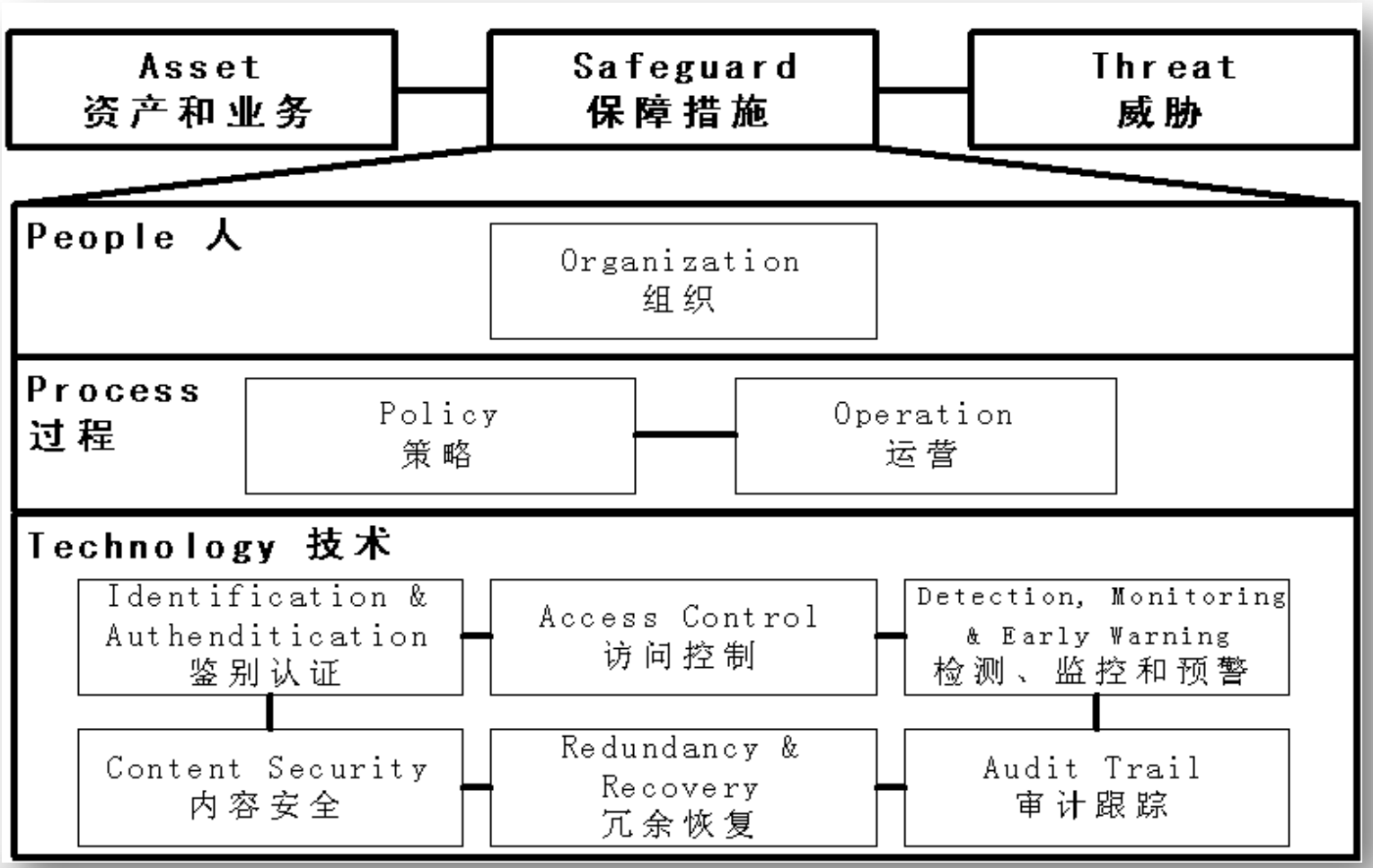
资产和业务
Asset

保障措施
Safeguard

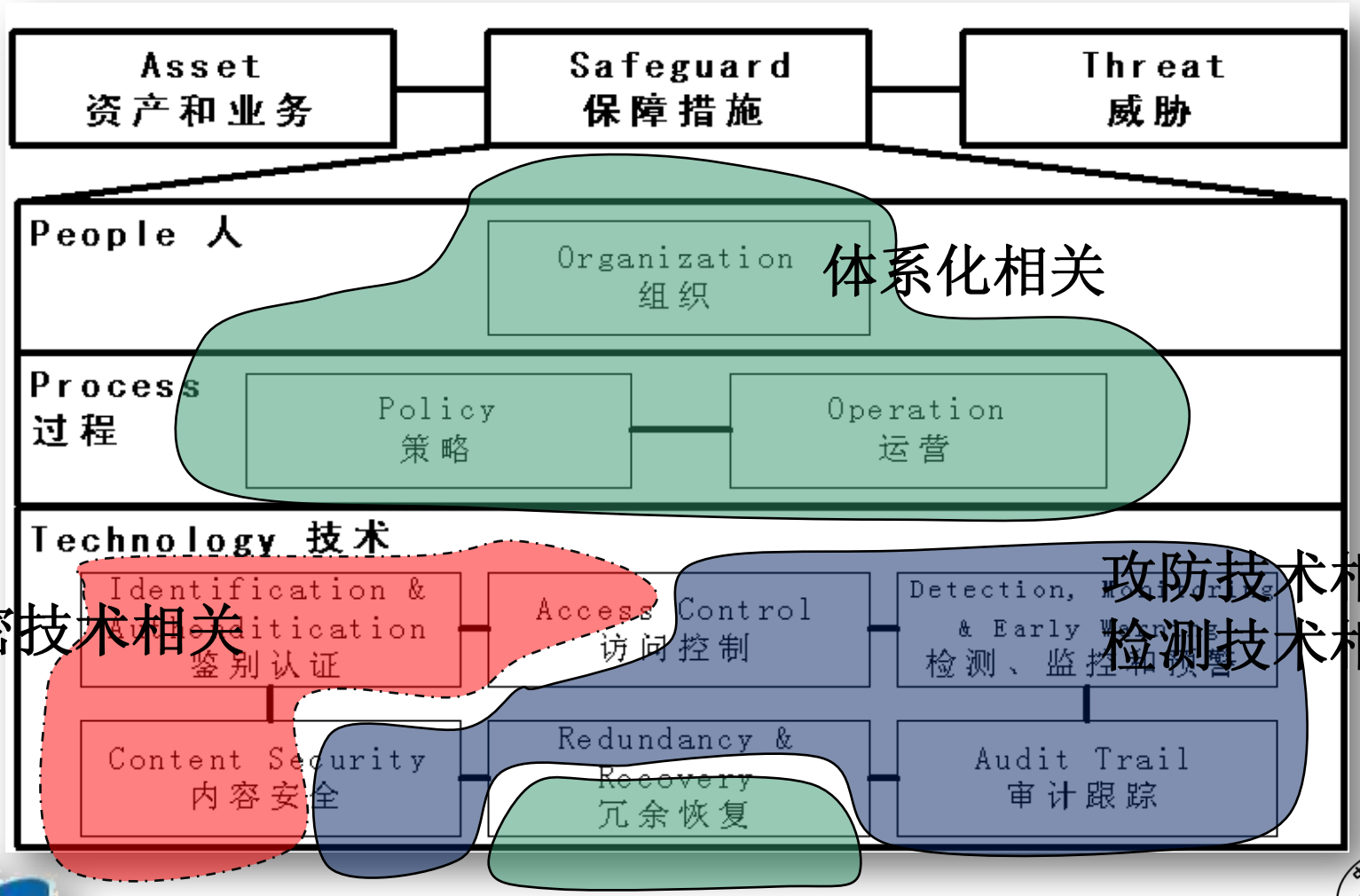
威胁
Threa



S 信息安全保障框架

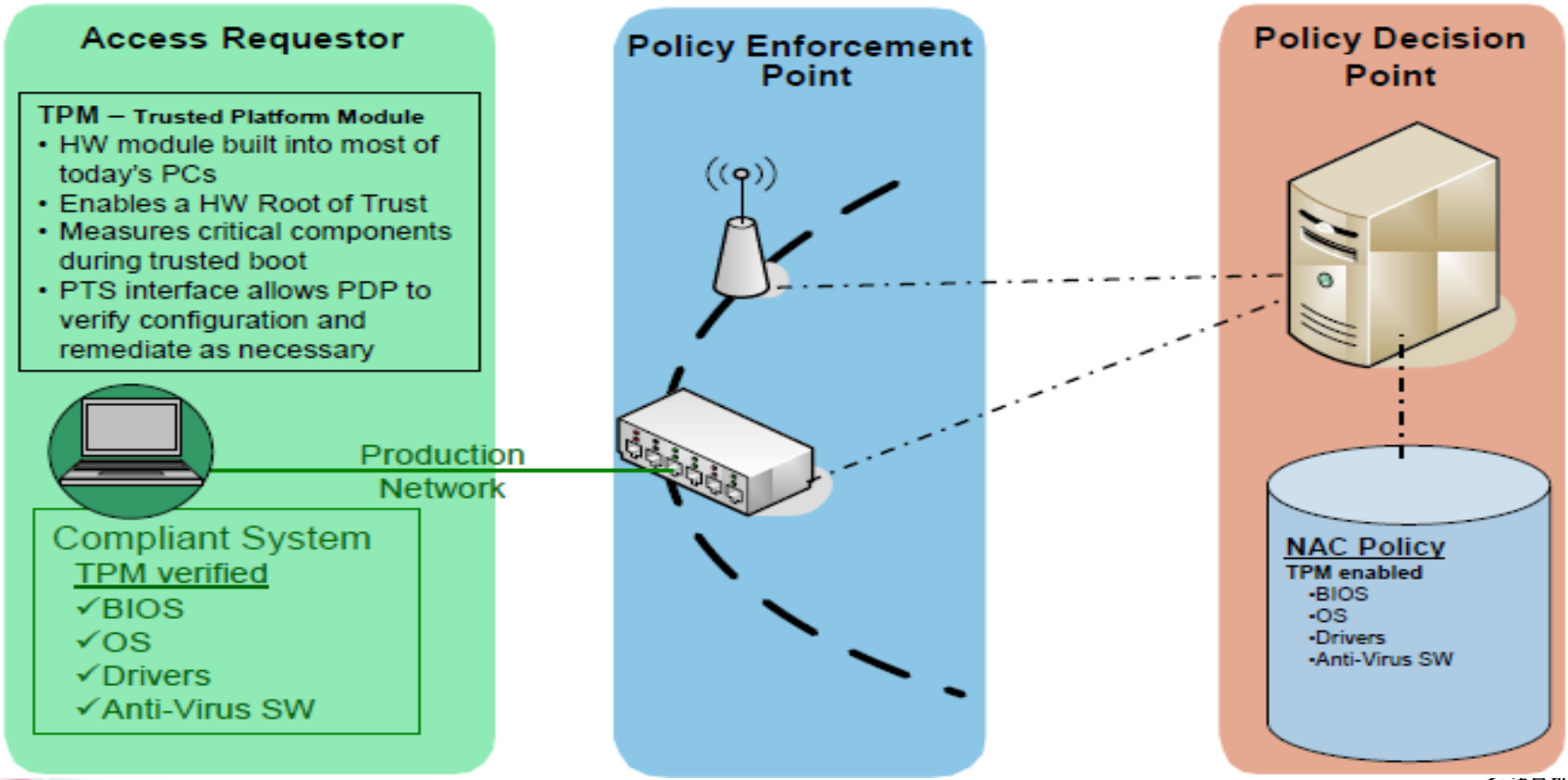

Asset
资产和业务
Safeguard
保障措施
Threat
威胁
People 人
Organization
组织
Process
过程
Policy
策略
Operation
运营
Technology 技术
Identification & Authenditication
鉴别认证
Access Control
访问控制
Detection, Monitoring & Early Warning
检测、监控和预警
Content Security
内容安全
Redundancy & Recovery
冗余恢复
Audit Trail
审计跟踪

三类信息安全技术


Asset
资产和业务
Safeguard
保障措施
Threat
威胁
People 人
Organization
组织
体系化相关
Process
过程
Policy
策略
Operation
运营
Technology 技术
Identification &
鉴别认证
Access Control
访问控制
Detection,
& Early
检测、
攻防技术相关
检测技术相关
加密技术相关
Content Security
内容安全
Redundancy &
Recovery
冗余恢复
Audit Trail
审计跟踪

可信计算的风格特征

基于TPM的完整性检查



S 可信计算的风格特征

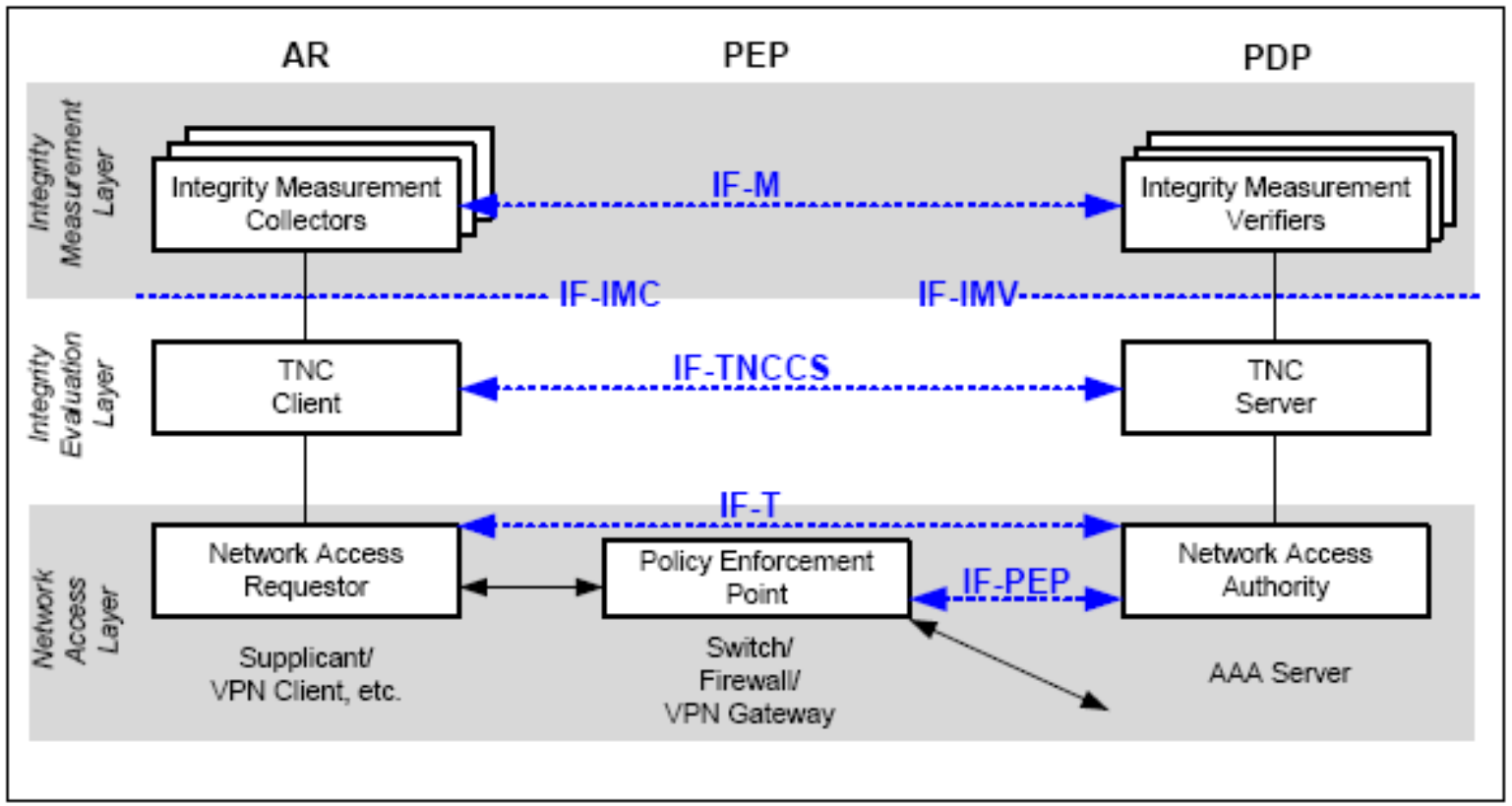
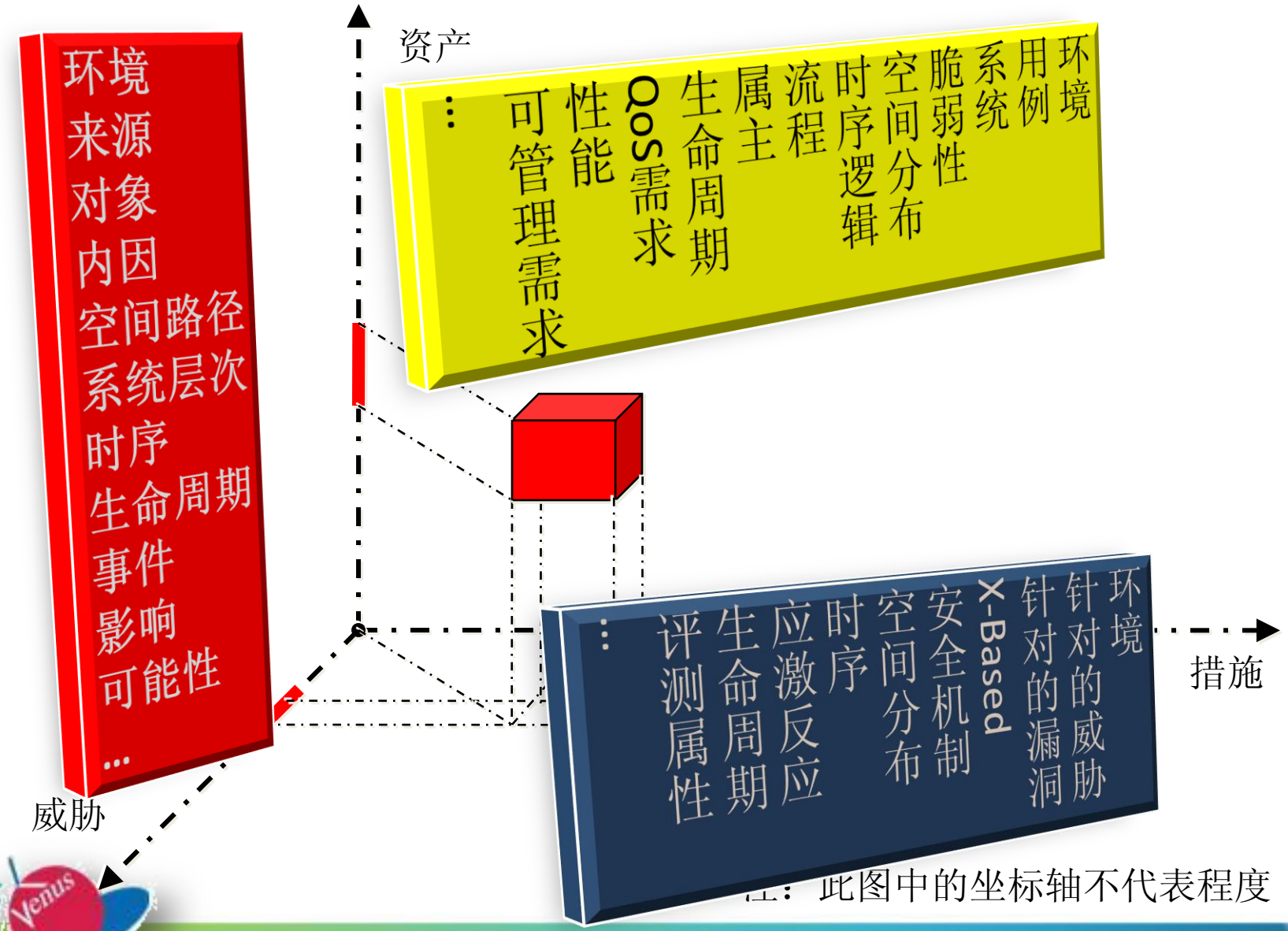


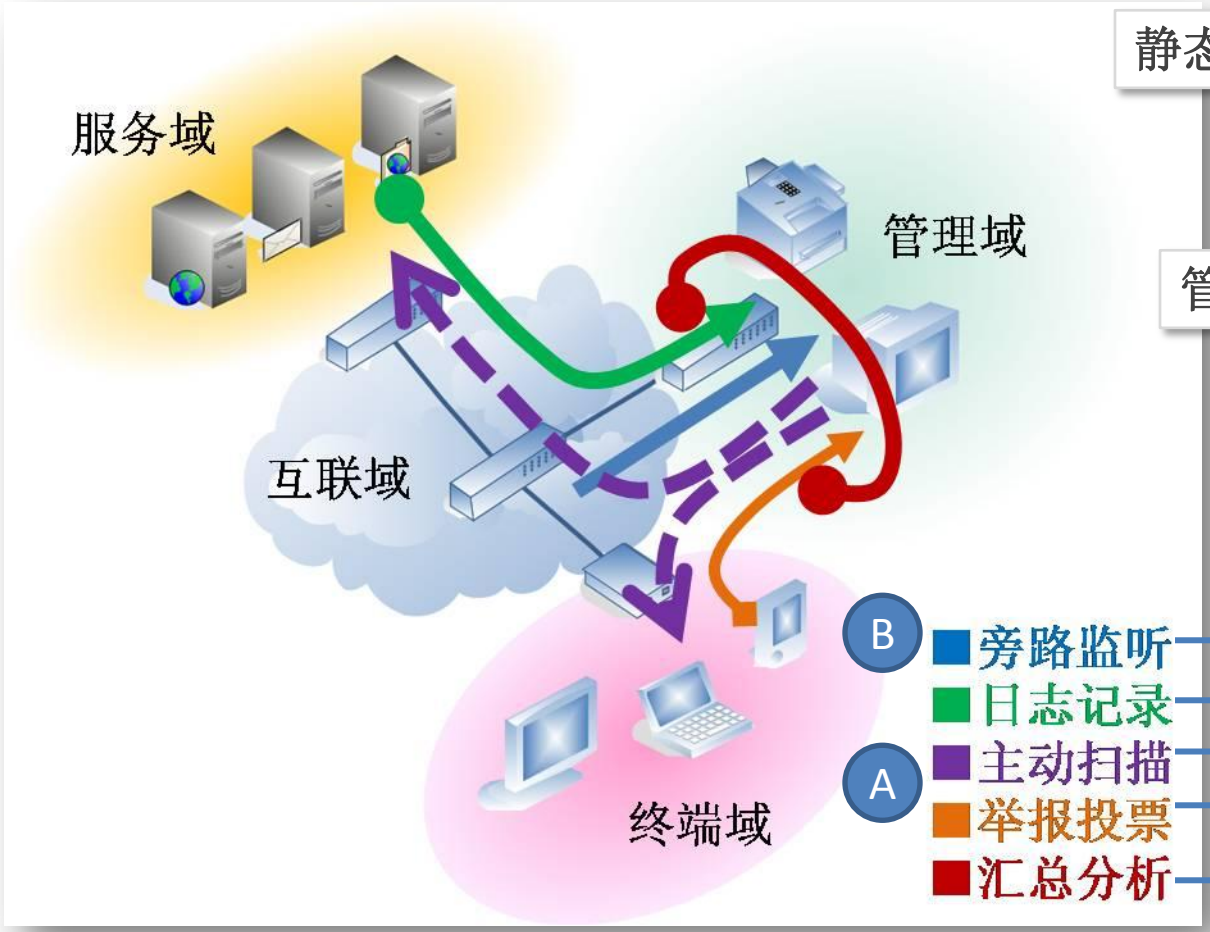
Figure 2: The TNC Architecture

所谓攻防就是流(过程)对抗



注：此图中的坐标轴不代表程度

S 检测的发展



静态数据体 → 病毒检测

C

代码 → 代码检查

管理体系 → 风险评估

S

合规测评

基于风险管理思想的体系化方法

国内的一些规章制度

- 等级保护
- 涉密分级保护
- 风险评估和安全检查
- 行业性规定

IT治理的三大标准

- 业务连续性管理 — BS25999
- IT服务管理 — ISO20000
- 信息安全管理 — ISO27001

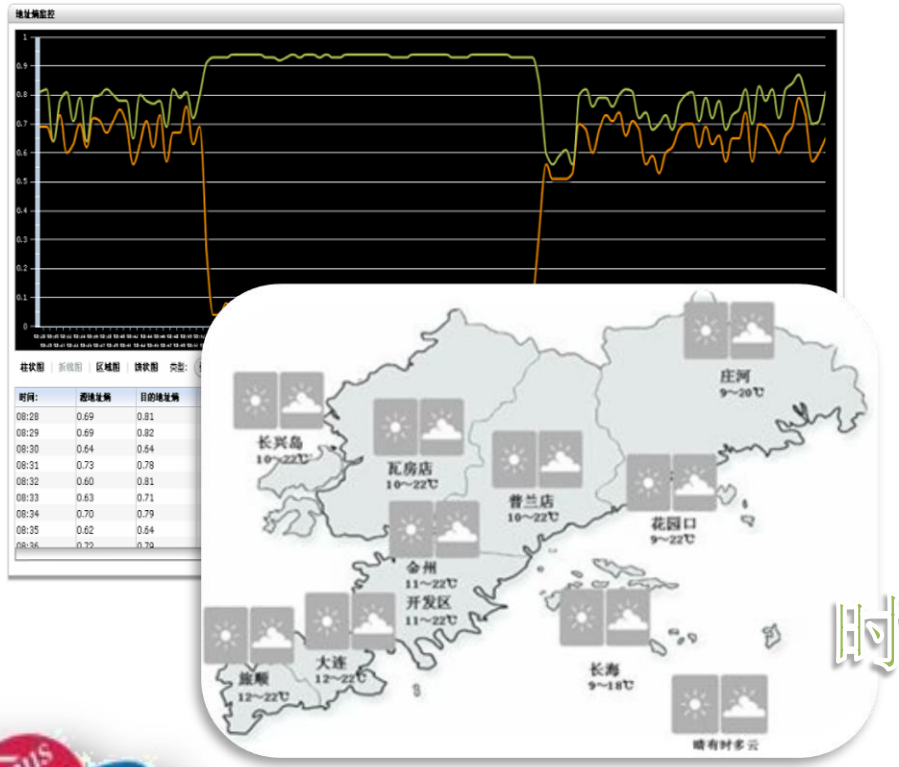
风险管理的高级宏观微观问题

高级的评估和高级的处置

宏观

全局预警——宏观态势感知

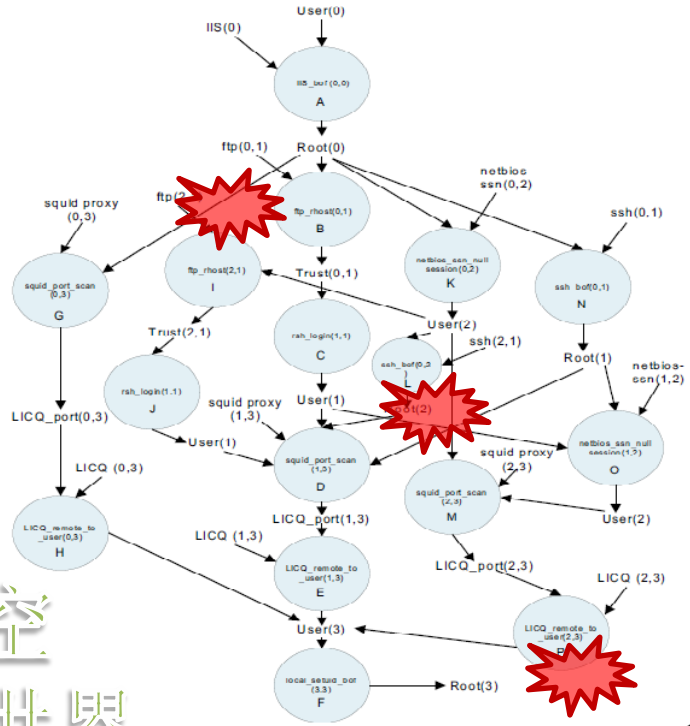
- 难点是看不全



微观

动态预防——APT防范

- 难点是看不见



时空

世界

宇宙

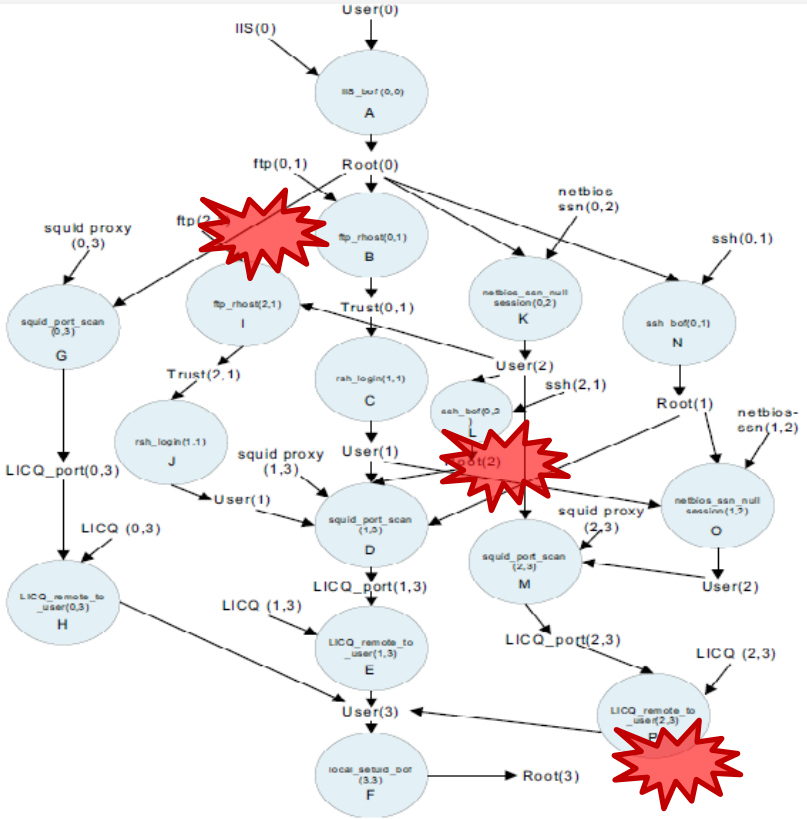
风险管理微观问题

微观

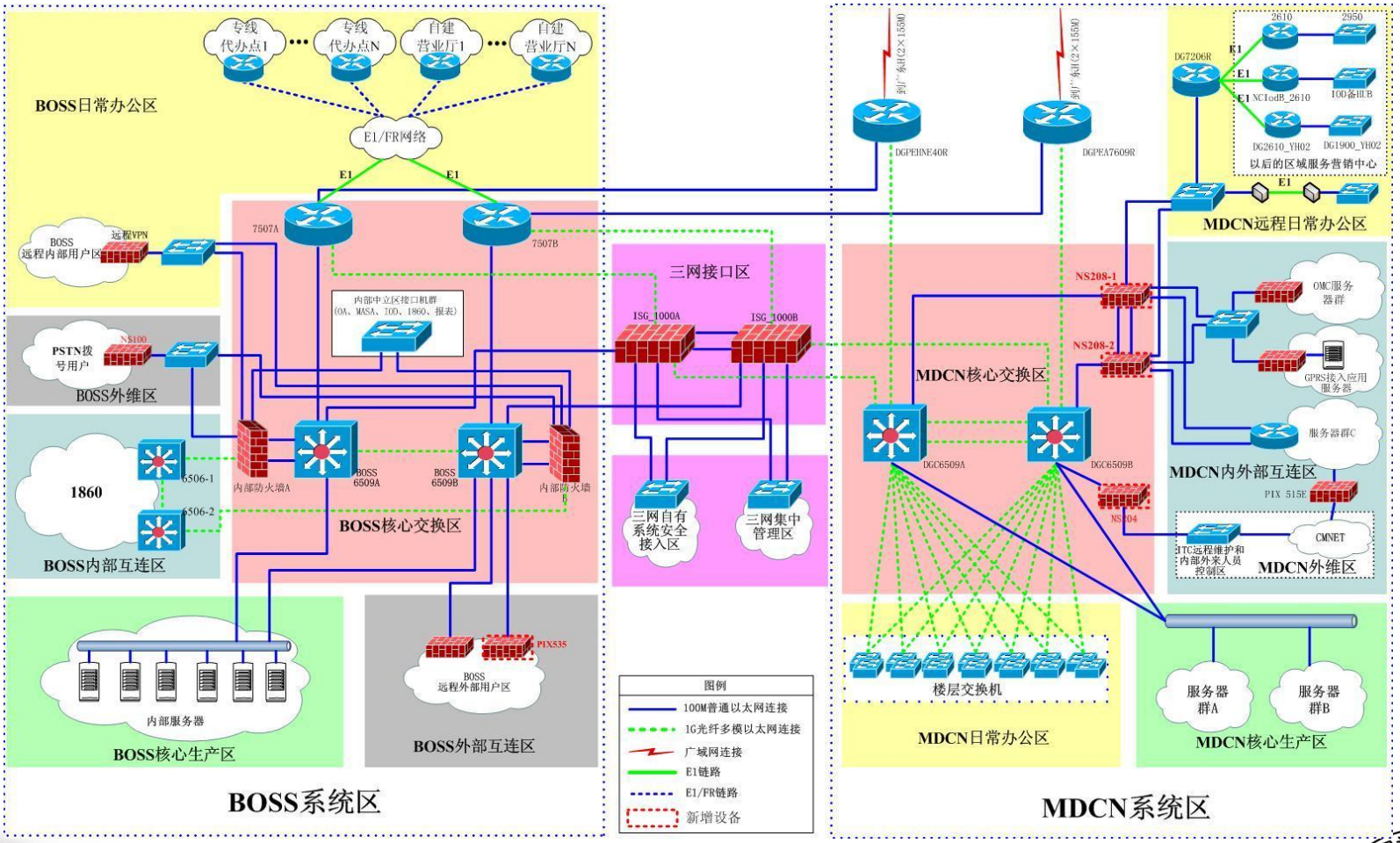
管控思维

- A
  - 明确价值关注对象，即被保护目标
  - 分解被保护目标的结构
    - **安全域**描述对象及其所在环境
    - **业务流和数据流**(Use-Case)表达业务的活动情态
- T
  - 用**威胁用例**(Threat-Case)表达威胁
- S
  - 落地在技术和管理的**管控措施**上

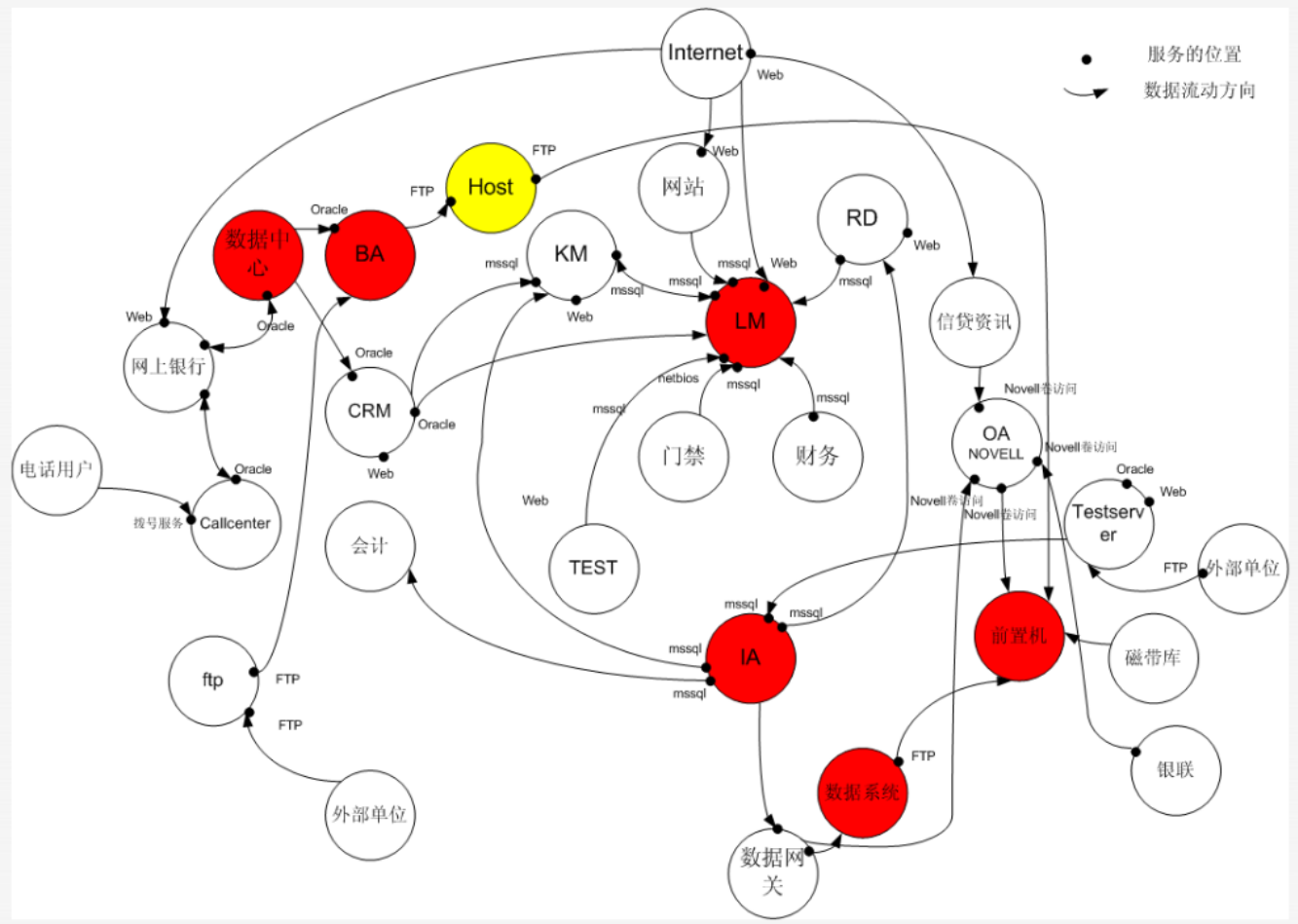
流的观点 X-Case



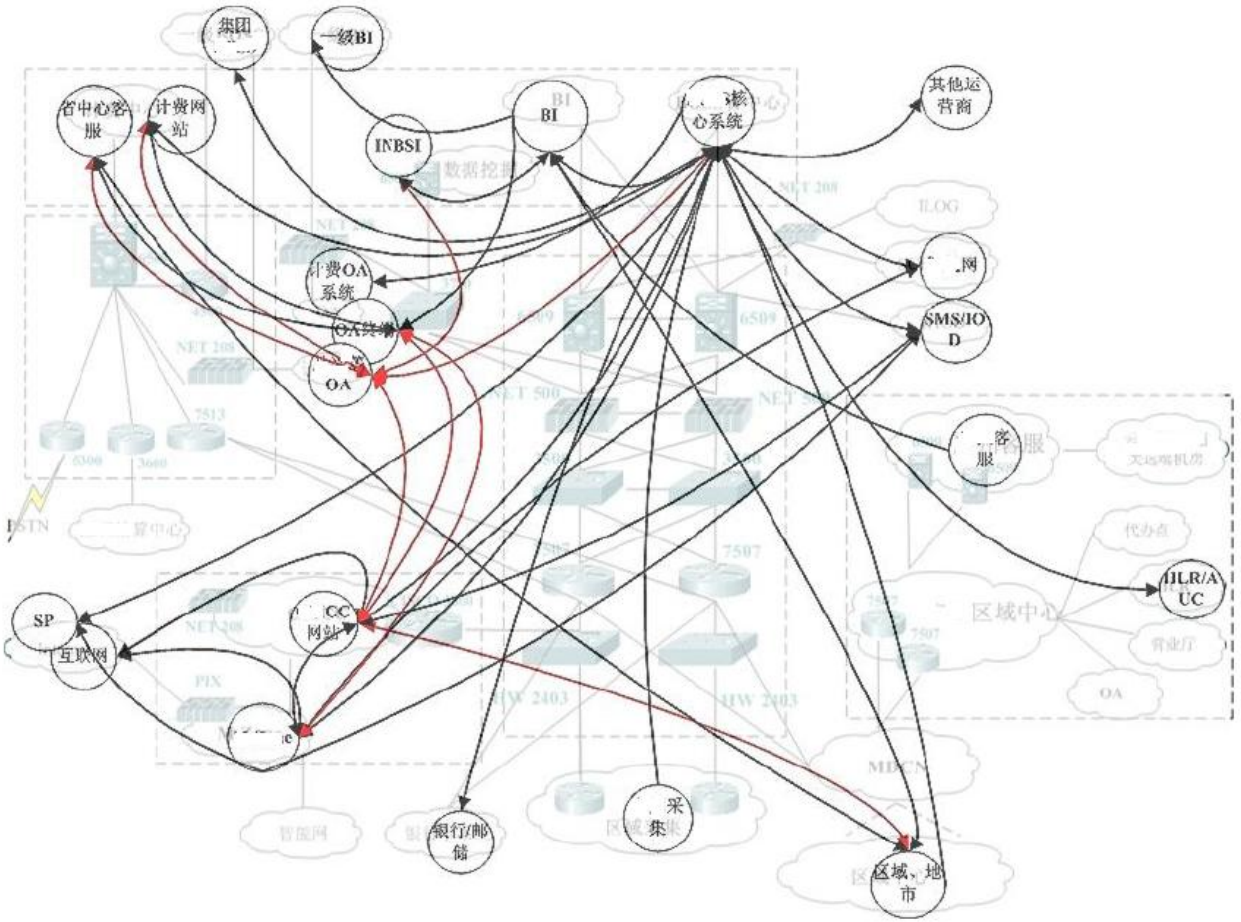
A 安全域、网络结构


BOSS日常办公区
专线代办点1
专线代办点N
自建营业厅1
自建营业厅N
E1/FR网络
E1
E1
BOSS远程内部用户区
远程VPN
7507A
7507B
内部中立区接口机群
(OA、WASA、TOD、1860、报表)
三网接口区
ISG_1000A
ISG_1000B
PSTN拨号用户
NS100
BOSS外维区
1860
6506-1
6506-2
BOSS内部互连区
内部防火墙A
BOSS 6509A
BOSS 6509B
内部防火墙B
BOSS核心交换区
三网自有系统安全接入区
三网集中管理区
内部服务器
BOSS核心生产区
PIX535
BOSS远程外部用户区
BOSS外部互连区
BOSS系统区
图例
100M普通以太网连接
1G光纤多模以太网连接
广域网连接
E1链路
E1/FR链路
新增设备
DGPEHNE40R
DGPEA7609R
DG7206R
2610
2950
NCIodB_2610
IOD备HUB
DG2610_YH02
DG1900_YH02
以后的区域服务营销中心
MDCN远程日常办公区
NS208-1
NS208-2
MDCN核心交换区
DGC6509A
DGC6509B
NS204
楼层交换机
MDCN日常办公区
OMC服务器群
GPRS接入应用服务器
服务器群C
MDCN内外部互连区
PIX 515E
ITC远程维护和内部外来人员控制区
CMNET
MDCN外维区
服务器群A
服务器群B
MDCN核心生产区
MDCN系统区

A 业务流


Internet
Web
服务的位置
数据流动方向
网站
Host
FTP
数据中心
Oracle
BA
KM
mssql
RD
Web
LM
信贷资讯
网上银行
CRM
netbios
门禁
财务
Novell卷访问
OA NOVELL
电话用户
拨号服务
Callcenter
会计
TEST
Testserver
外部单位
IA
前置机
磁带库
ftp
外部单位
数据系统
银联
数据网关

A 网络结构和业务流构成地图



威胁场景/威胁用例/广义威胁

- 威胁的环境Environment：前提、假设、条件等
- 威胁的来源Agent：包括攻击者、误用者、故障源、自然（灾害）等
- 威胁的对象Object：攻击目标和破坏对象，也就是要被保护的对象
- 威胁的内因——脆弱性Vulnerability：自身保护不当的地方
- 威胁的过程Process
  - 威胁的途径Route：指威胁必须通过才能[illegible]通过网络、要在物理上接近设备
  - [illegible]的步骤和顺序。与威胁的途径是一[illegible]表达。也可以将这两个因素结合起来表达威胁

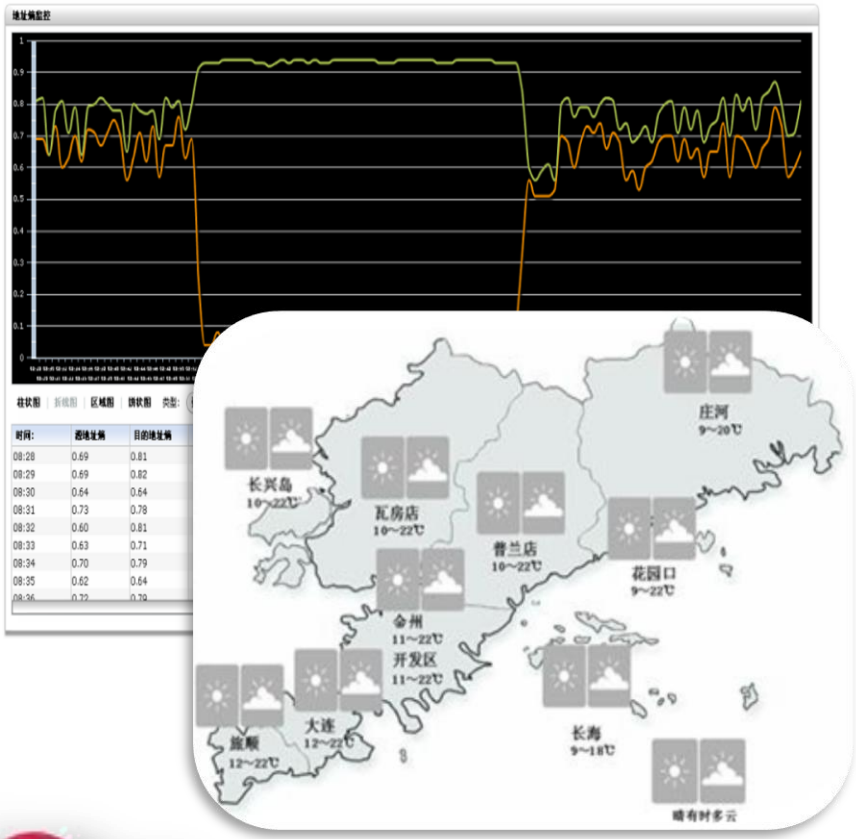
APT检测就是要勾勒出复杂的威胁用例

- 威胁的结果——事件Event/Incident：威胁具体实现之后所造成的结果
  - 威胁的可能性：威胁产生结果变成事件的概率。
  - 威胁的影响范围：威胁产生结果后的影响大小。以及影响进一步扩散的特性。

风险管理宏观问题

宏观

空间



秩序和治理

- 多方参与的CyberSpace
- 社会性、宏观经济性、基础设施
- IT地图
- 群落内部和群落间的交互影响

A

- 关注有宏观影响的危害
  - 正反馈自激震荡效果
  - 关键基础设施的破坏，业务流的共性颈环节，如DNS
  - 大规模群体参与，如僵尸网

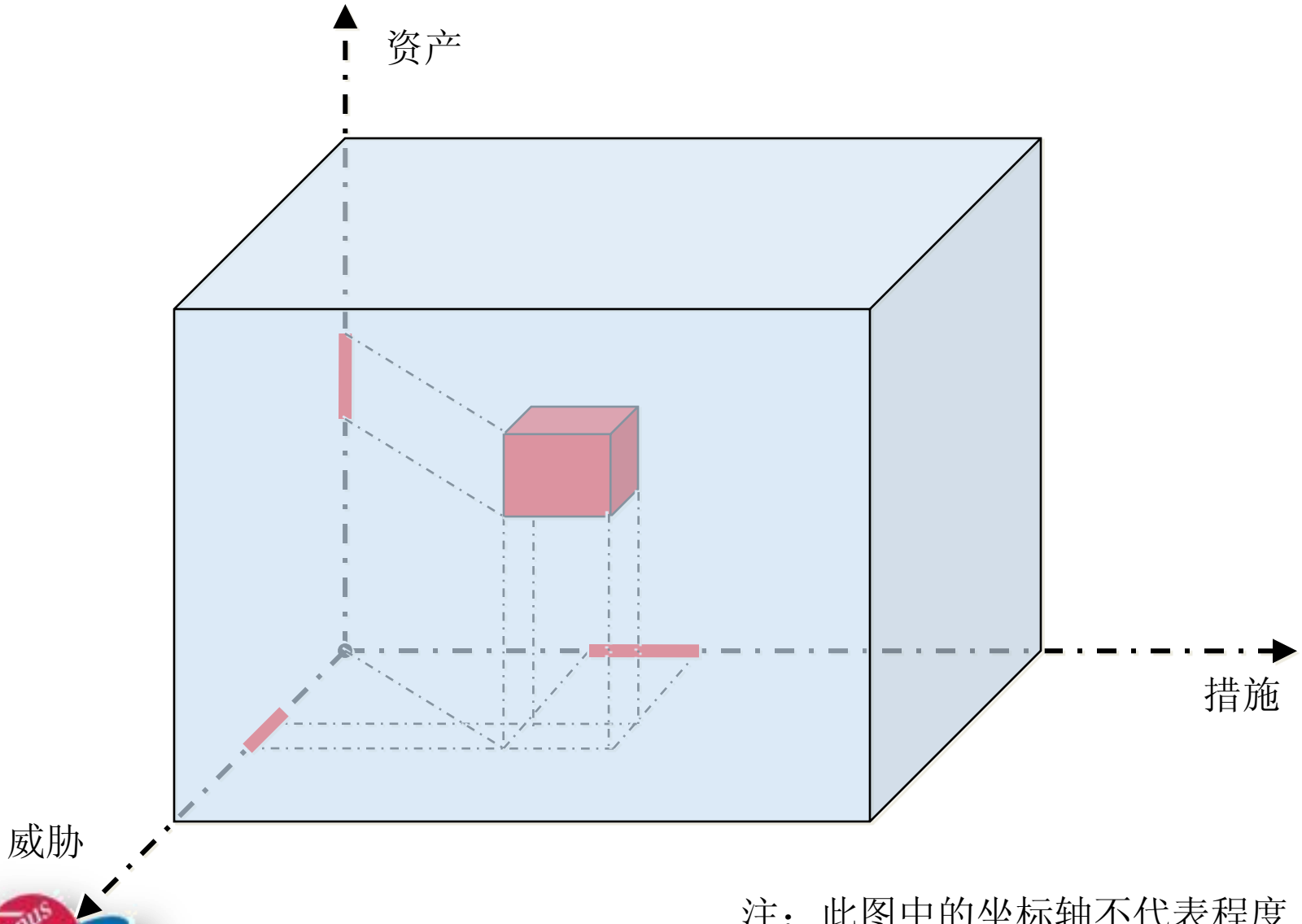
T

- 从管控到治理
- 以秩序作为治理的基础
- 宏观指标的提炼，反馈或前馈关系

S

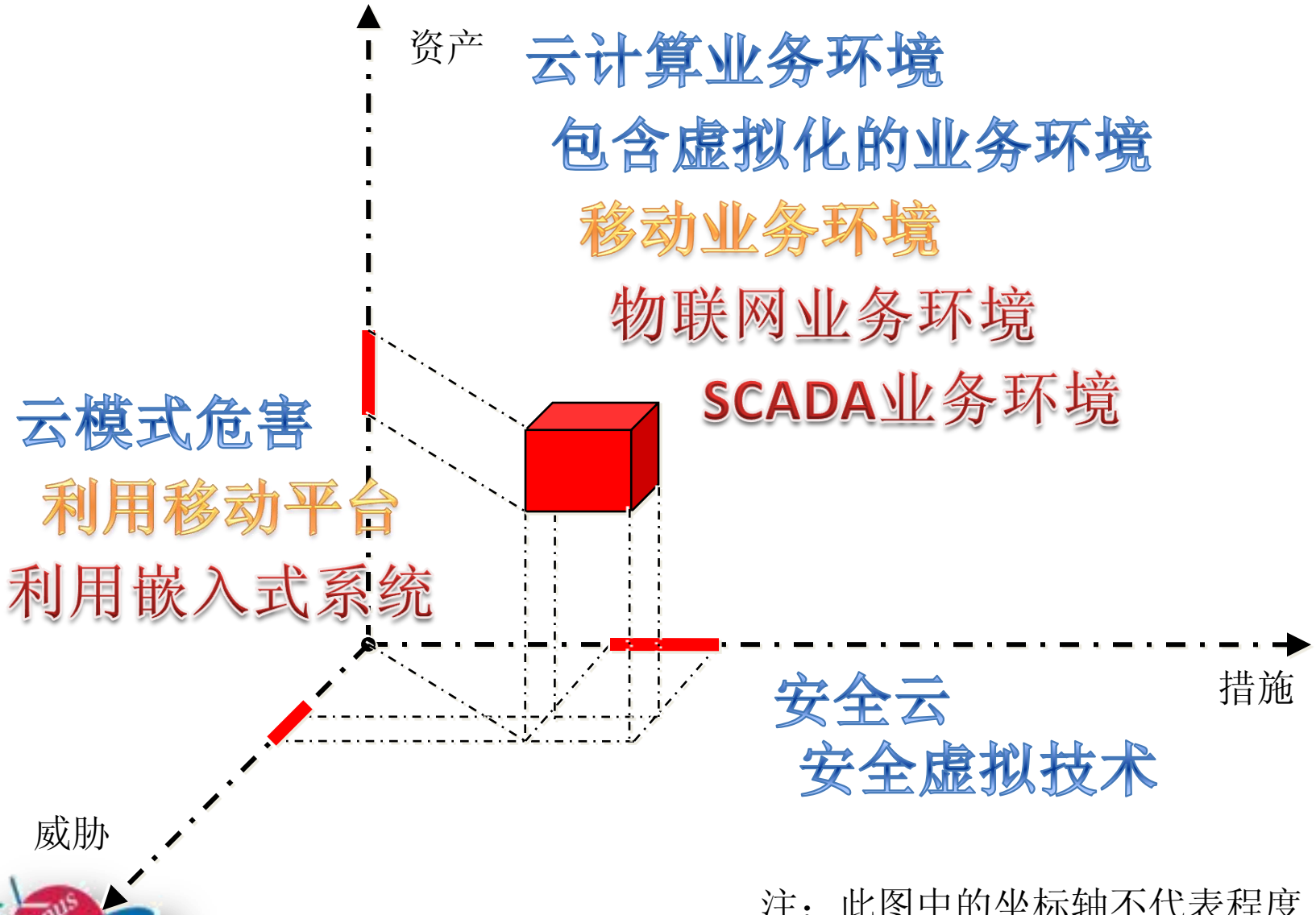
所谓新计算对风险管理的影响

风险立方体中的安全工作



注：此图中的坐标轴不代表程度

新计算作用于风险立方体中



注：此图中的坐标轴不代表程度

云模式——水性、砂性

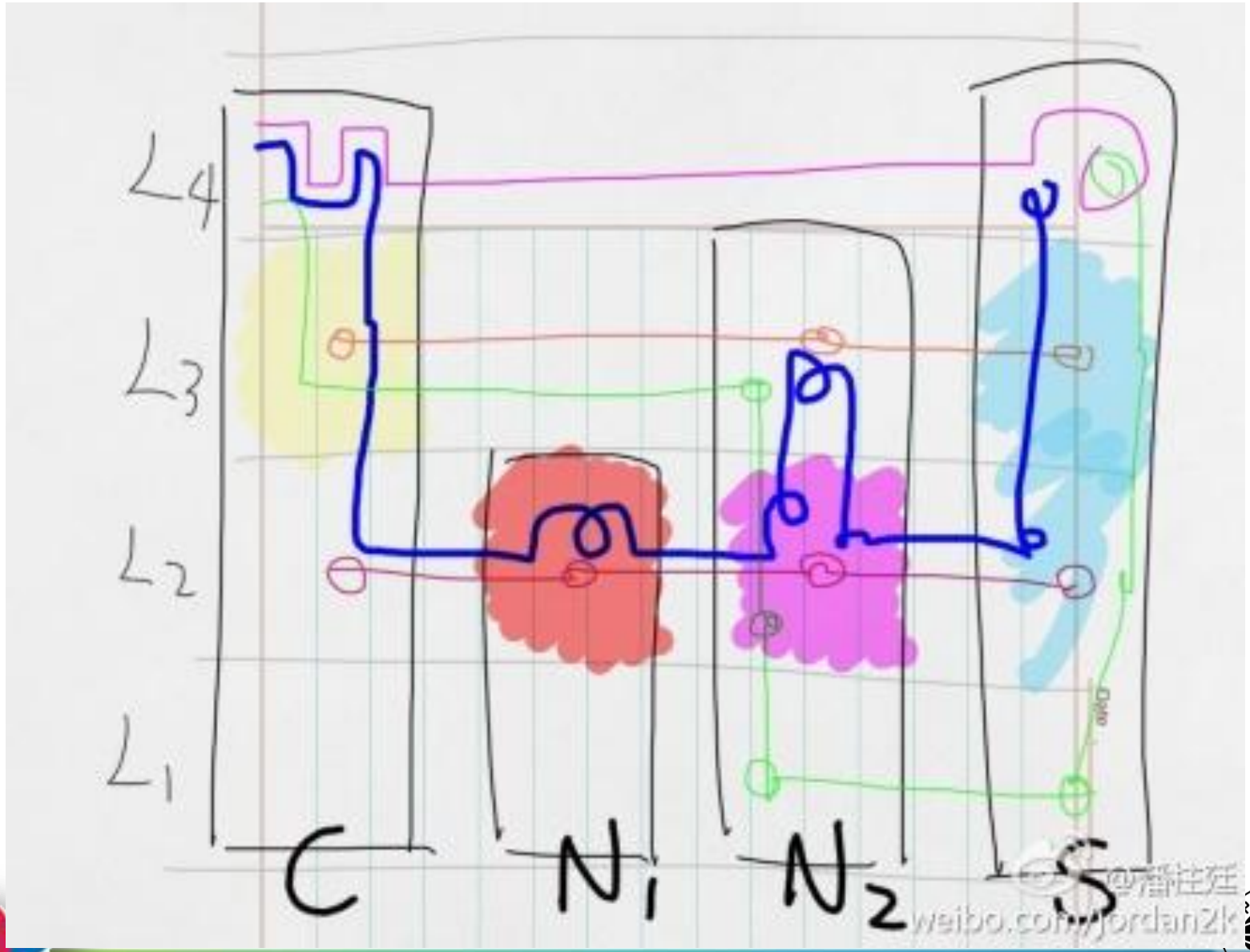

根本物质
• 水
• 服务
源
• 海、湖、河、地表
• 实际资源
云朵形成
• 形成虚拟资源
传输体系
• 大气环流
• 网络、通信
云朵接触
• 虚拟资源前端
成雨条件
• 客户端、访问
降水
• 获得水
• 获得云服务
用水
• 本地水处理和应用
• 服务再加工

虚拟化对于安全功能的拆解

部署于 安全功能 作用于

部署于 \ 作用于	虚拟层	虚拟平台	实体层
虚拟层			
虚拟平台			
实体层			

客观存在的业务流和域



风险管理的流

管控思维下的流

A
- 明确价值关注对象，即被保护目标
- 分解被保护目标的结构
  - **安全域**描述对象及其所在环境
  - **业务流和数据流**(Use-Case)表达业务的活动情态

T
- 用**威胁用例**(Threat-Case)表达威胁

S
- 落地在技术和管理的**管控措施**上

治理思维下的流和势

微观

A
- 多方参与的CyberSpace
- 社会性、宏观经济性、基础设施
- IT地图
- 群落内部和群落间的交互影响

宏观

T
- 关注有宏观影响的危害
  - 正反馈自激震荡效果
  - 关键基础设施的破坏，业务流的共性颈环节，如DNS
  - 大规模群体参与，如僵尸网

S
- 从管控到治理
- 以秩序作为治理的基础
- 宏观指标的提炼

RSA CONFERENCE CHINA 2011
2011 信息安全国际论坛

the adventures of alic & bob

风险管理 新兴计算 流观/过程观

潘柱廷

@启明星辰 首席战略官 http://www.venustech.com.cn

@中国计算机学会 理事 http://www.ccf.org.cn

@云安全联盟中国区 理事 http://www.csagcc.org

pan_zhuting@venustech.com.cn

jordan@venustech.com.cn

博客：http://blog.sina.com.cn/jordan2k

微博：http://weibo.com/jordan2k