# 信息物理系统（CPS）安全技术研究

中国电子技术标准化研究院

# 大纲

一、信息物理系统简介

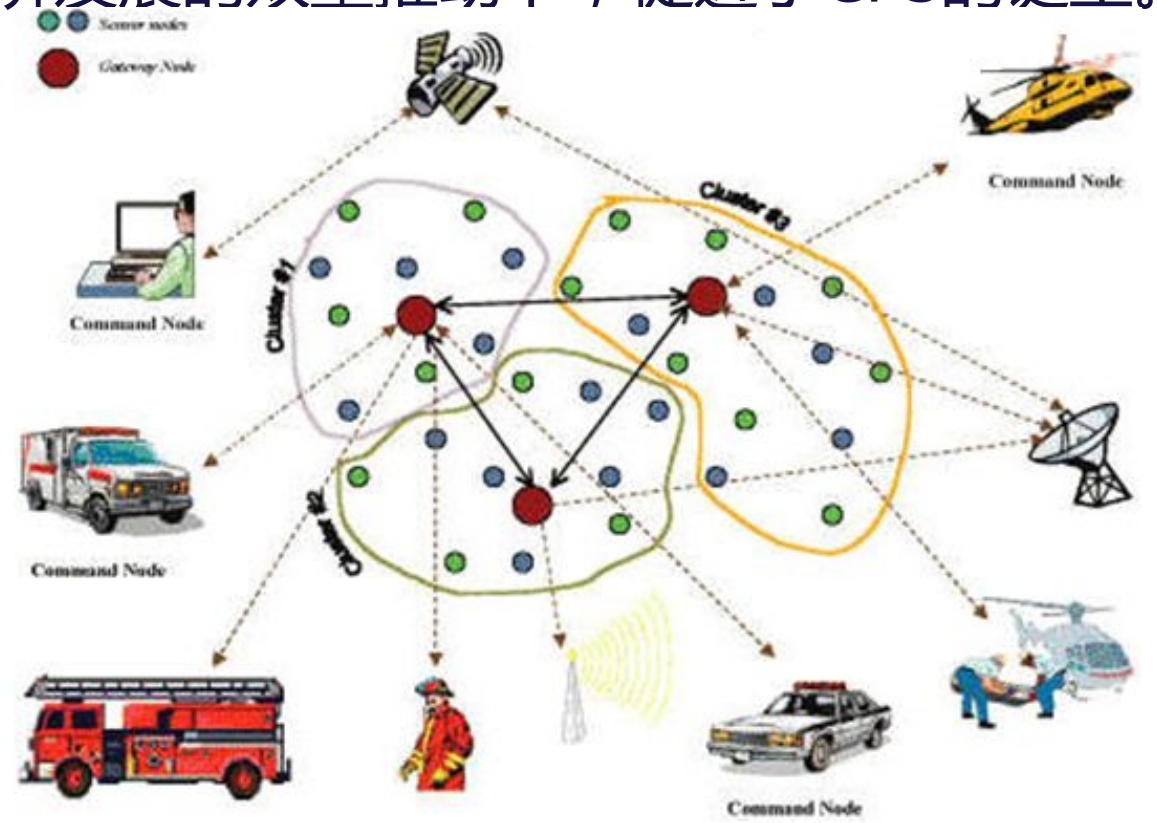
二、信息物理系统信息安全

三、信息物理系统信息安全测评

# 一、信息物理系统简介

## CPS产生的背景

- 当前，网络信息技术的飞速发展以及和工业领域的深度融合，科技与经济发展的双重推动下，促进了CPS的诞生。



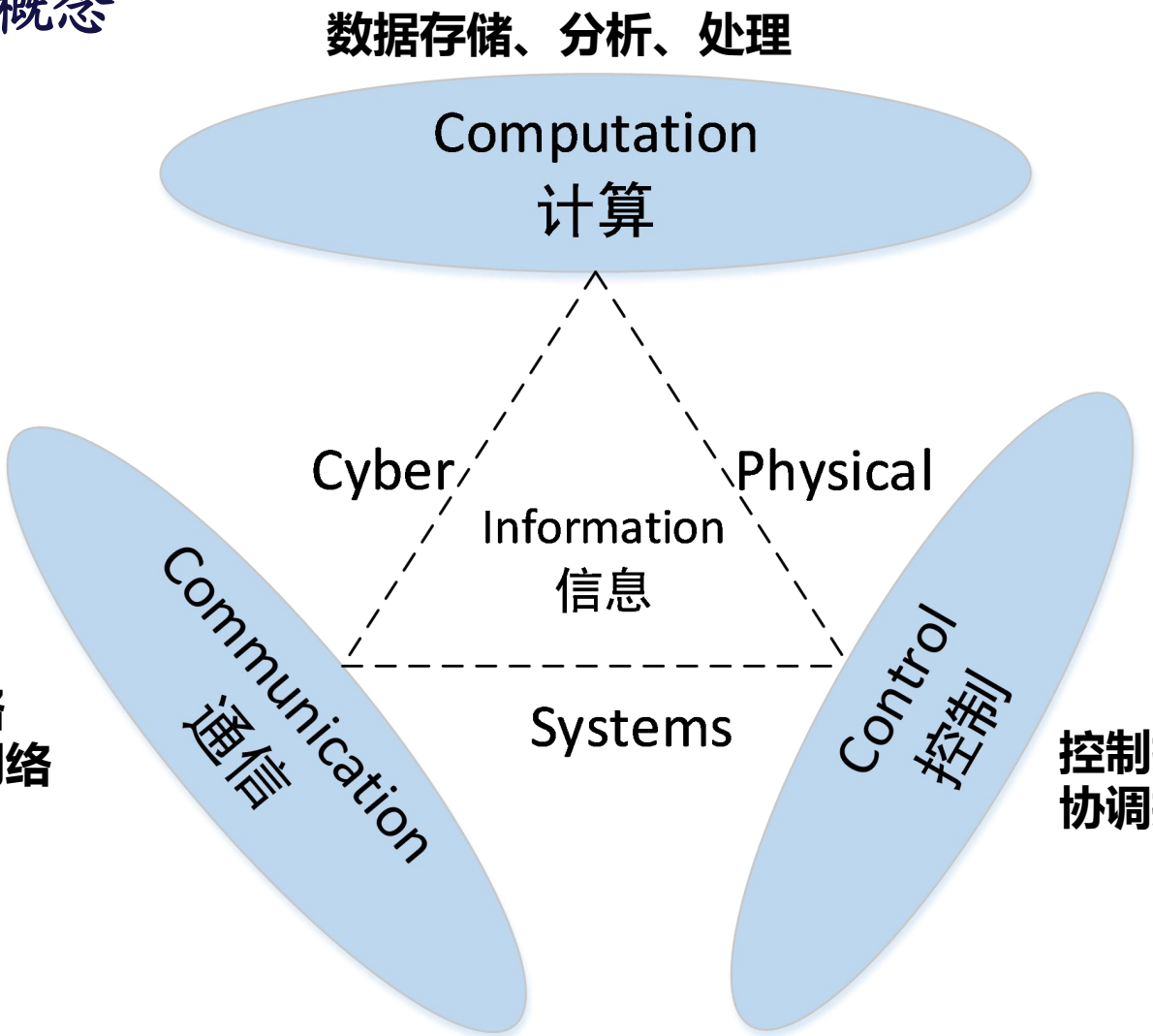
# 一、信息物理系统简介

## CPS产生的背景

- CPS最早在2006年美国政府发布的《美国竞争力计划》中提出，同年10月，美国国家自然科学基金会（Nation Science Foundation, NSF）将CPS列为美国未来八大关键信息技术的首位.
- 2010年美国总统科技顾问委员会明确将其列为美国政府应当优先关注的技术之一。
- 德国政府2011年11月公布的《高技术战略2020》中的一项重要战略是工业4.0，其中核心之一是通过CPS开创新的制造方式，实现“智能工厂”。
- 中国在2012年《十八大报告》突出强调‘‘推动信息化和工业化深度融合，加快传统产业转型升级”。
- 2013年10月，工业和信息化部以工信部信[2013]317号文印发《信息化和工业化深度融合专项行动计划（2013-2018年）》。
- 2014年10月，中德双方举行的第三轮中德政府协商后发表的《中德合作行动纲要》中宣布，两国将开展“工业4.0”合作，而工业4.0的核心就是构建CPS。

# 一、信息物理系统简介

## CPS的核心概念




传感器网络
泛在通信网络

控制执行器
协调控制

# 一、信息物理系统简介

## CPS的组成

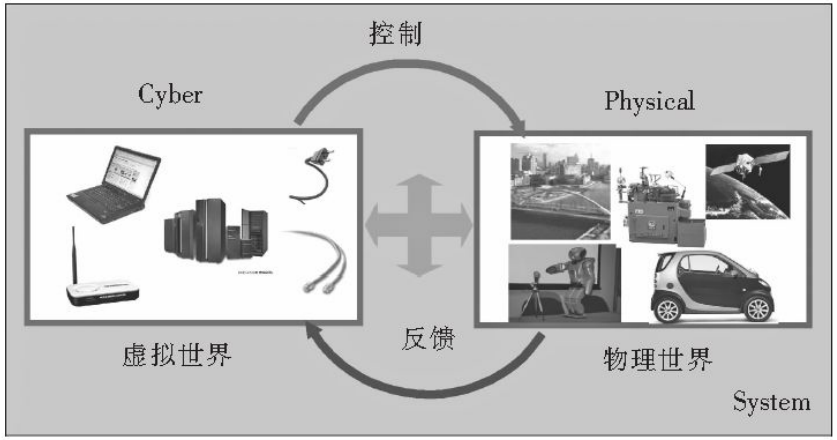



图 1　信息世界与物理世界交互示意图

CPS的通信网络可以逻辑地视为由传感器网络、执行器网络、计算机网络构成的组合通信网络。

CPS由传感器节点、执行器节点、传感器与执行器组合节点、计算系统和控制系统等组成。

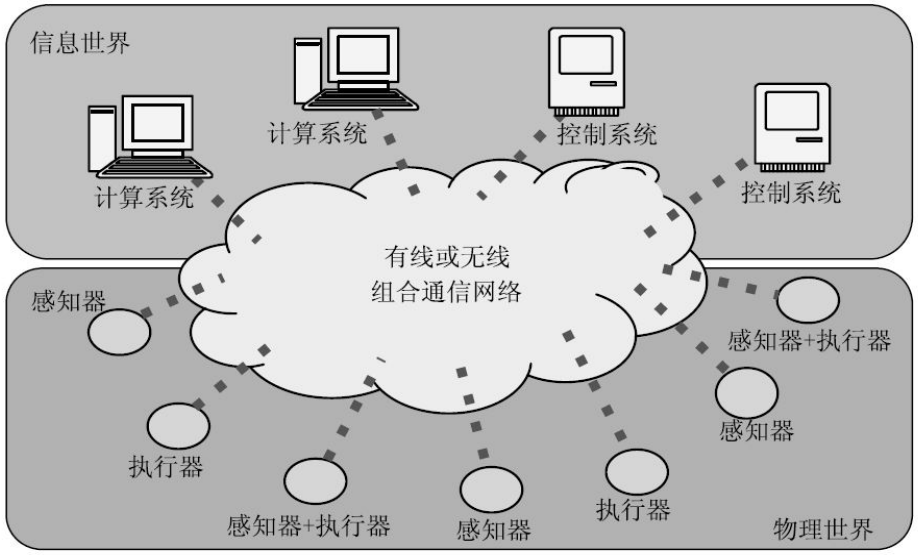
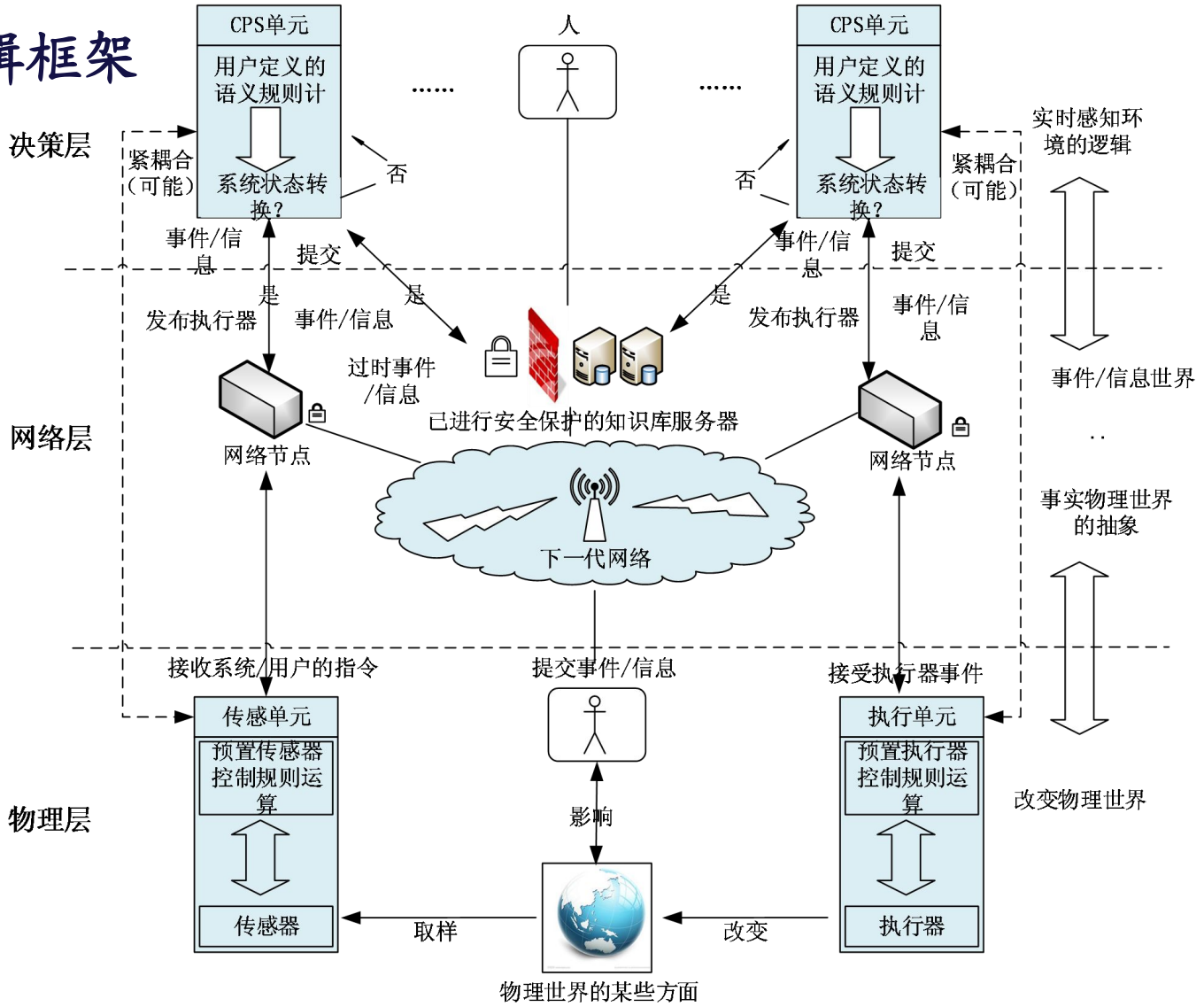



图 2　CPS 逻辑示意图

# 一、信息物理系统简介

## CPS的典型逻辑框架



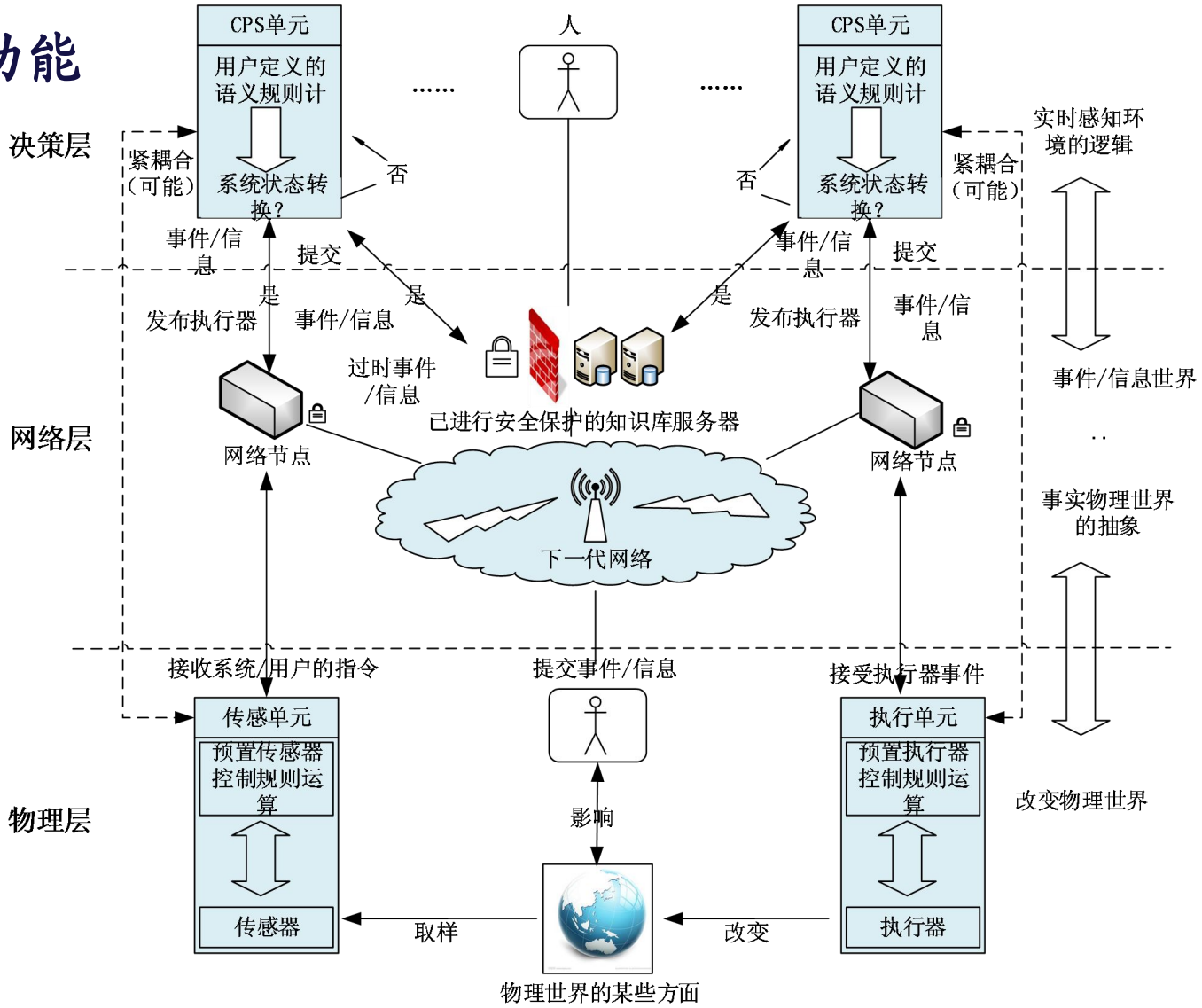
# 一、信息物理系统简介

## CPS基本逻辑功能

实时处理
智能控制

可靠传输

全面感知



# 一、信息物理系统简介

## CPS相关子系统

# 一、信息物理系统简介

## 软件密集系统

- **概念：系统中的软件在系统研制费用、研制时间或系统功能特性等一个或多个方面占主导地位的系统。**
- **特点：面向信息、面向知识。**
- **发展难点：随着软件密集系统规模的增长，其可靠性问题逐渐凸显，成为限制其发展的难点。**

# 一、信息物理系统简介

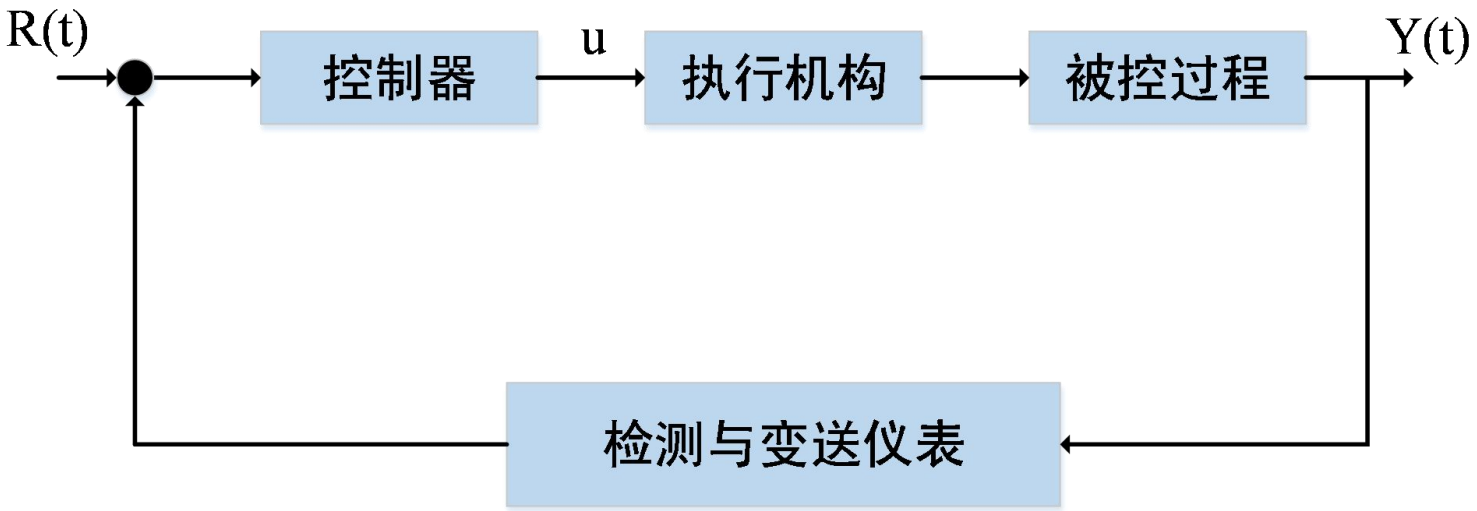
## 软硬件综合系统

- **概念：基于微电子技术和嵌入式技术，实现信息共享、系统集成和智能化控制的系统。**
- **特点：其软硬件均面向特定应用对象和任务设计，具有很强的专用性。**
- **系统失效原因：软硬件综合系统失效，通常是软件失效和硬件失效耦合的结果。**

# 一、信息物理系统简介

## 过程控制系统

- **概念：以表征生产过程的参量为被控制量，使之接近给定值或保持在给定范围内的自动控制系统。**
- **特点：一般过程控制系统通常采用反馈控制的形式。**
- **系统组成如下图所示：**



# 一、信息物理系统简介

## 物联网

- **概念：通过RFID、红外感应器、全球定位系统等信息传感设备，按约定协议，将物品与互联网相连，进行信息交换和通信。**
- **特点：物与物相连、人与物相连、人与人相连，关键在于互联互通。**
- **物联网的层次架构如下图所示：**

| | | | | | | |
|---|---|---|---|---|---|---|
| 应用层 | 远程监控 | 异地医疗 | 环境检测 | 智能家居 | 资源探测 | 信息检索 |
| 处理层 | 云计算 | | 网格计算 | | 并行计算 | |
| 传输层 | 无线传感网 | 互联网 | 移动网络 | 局域网 | 广电网络 | |
| 传感层 | 智能终端 | RFID设备 | 传感器节点 | 网关设备 | 移动设备 | |

# 一、信息物理系统简介

## 无线传感器网络

- **概念：由部属在监测区域内的大量卫星传感器节点构成，是通过无线通信方式组成的一个多跳自组织网络。**

- **特点：网络中的传感器以协作的方式感知、采集、处理和传输网络覆盖地理区域内被感知对象的信息，并最终把这些信息发送给网络的所有者。**

- **发展基础：MEMS、片上系统、无线通信和低功耗嵌入式技术。**

# 一、信息物理系统简介

## CPS主要特点

- 信息物理高度融合
- 系统功能交互涌现
- 系统结构动态演化
- 内外状态深度感知
- 网络实时适应控制

# 大纲

一、信息物理系统简介

二、信息物理系统信息安全

三、信息物理系统信息安全测评

# 二、信息物理系统信息安全

## CPS系统安全问题

信息物理系统所面临的安全性问题主要包括两种:

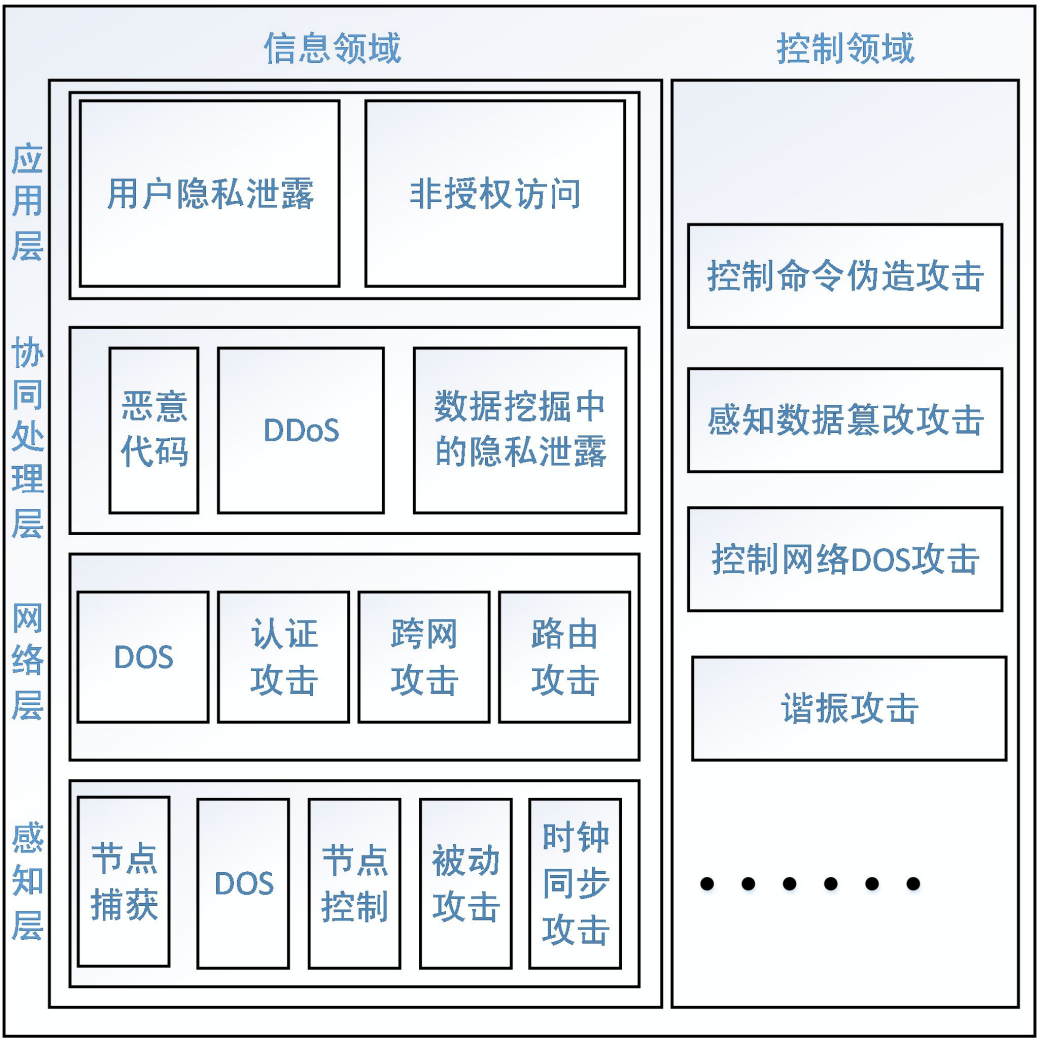
- 信息安全
- 物理安全

CPS系统中的安全要素包括:

- 威胁模型（不同类别的攻击);
- 检测方法（基于模型的、基于软件的或者数据驱动的）;
- 鲁棒性（攻击容忍性）;
- 恢复能力

# 二、信息物理系统信息安全

## CPS系统安全威胁




CPS系统所面临的安全威胁主要来自以下3个方面。

(1) CPS的感知层是由无线传感器网络构成的，大部分传感设备的通信、计算以及存储等能力十分有限，因此无法直接使用跳频通信以及公钥密码等传统安全机制。

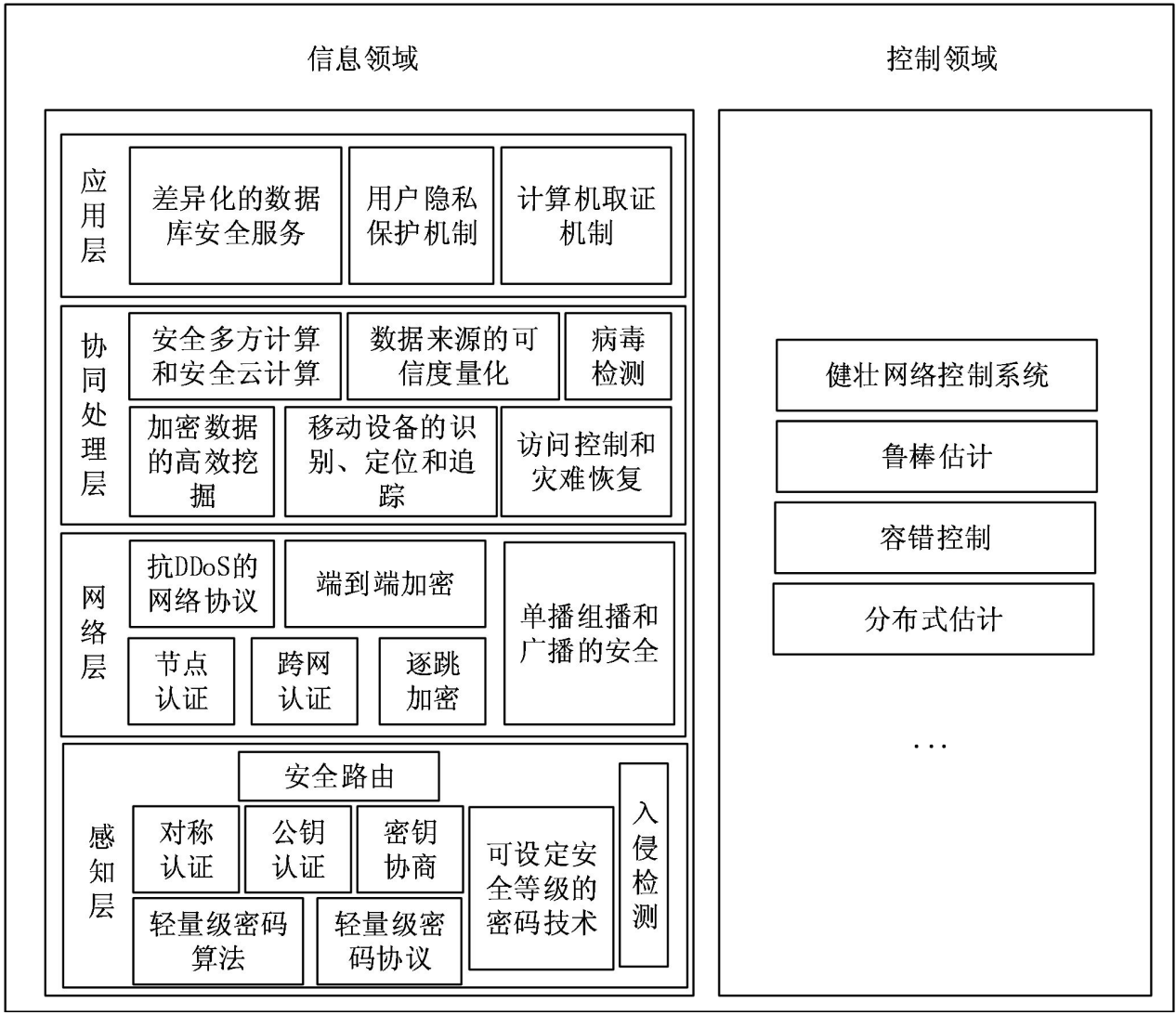
(2) 因为CPS系统利用未来网络作为核心承载网络，因此CPS系统的网络规模的增长和分布式的信息处理环境使得CPS系统网络更容易受到DoS攻击以及DDoS攻击。

(3) 因为CPS系统在控制系统中引入了网络特性，因此非法入侵者能够通过哄骗、阻塞、DoS攻击等方式使控制命令延迟或失真，从而导致CPS系统无法及时执行任务，甚至无法进入稳定状态。

# 二、信息物理系统信息安全

## CPS系统安全机制

当前对于CPS系统的安全研究和评估可分为信息安全和控制安全两个方面。信息安全方面的研究主要是解决在高混杂、大规模、协同自治的网络环境下信息的安全收集、处理和共享等问题。而控制安全方面主要集中解决在松散耦合、开放互连的网络化系统结构下的安全控制等问题。

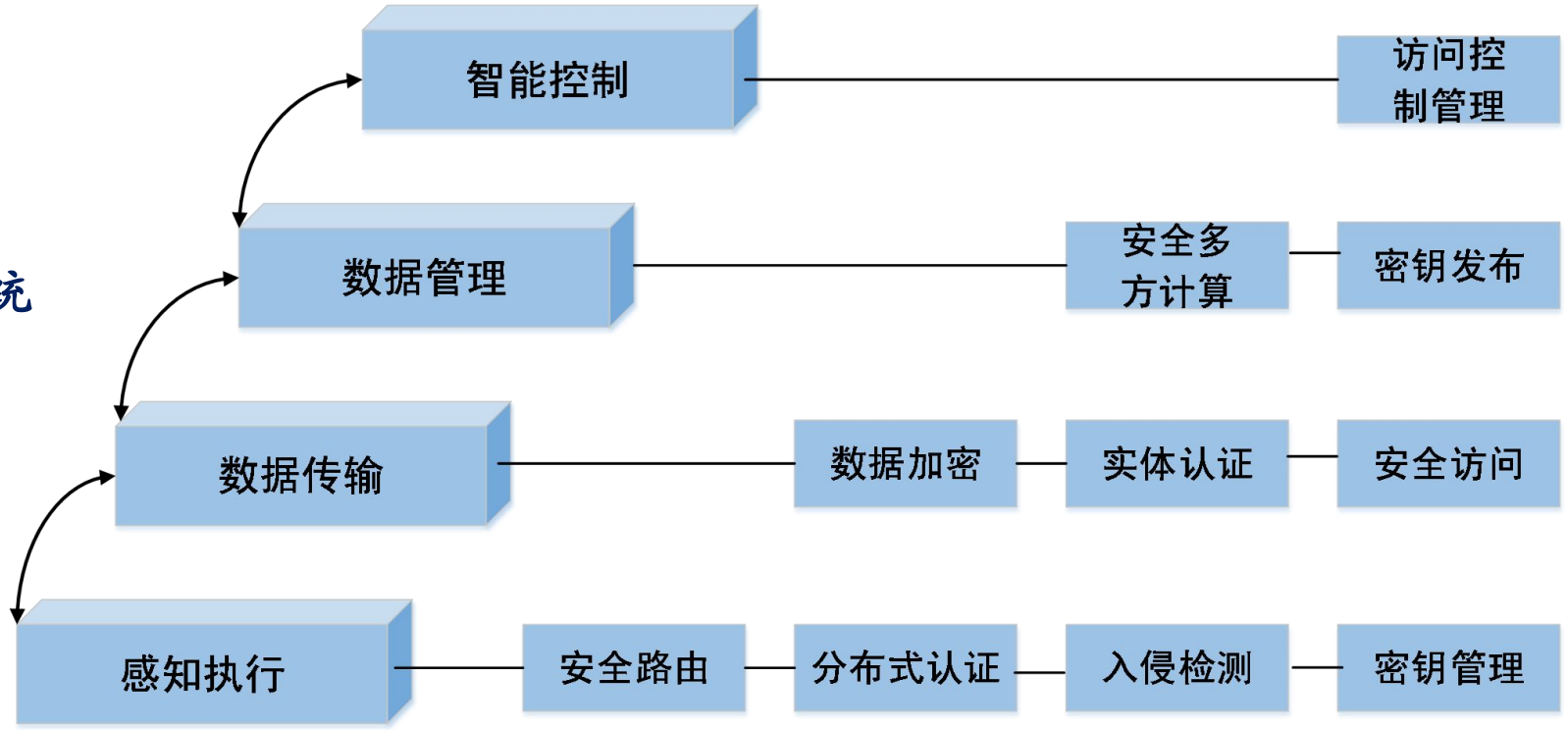


# 二、信息物理系统信息安全

## CPS系统安全架构

为了实现安全互联互通，提出了一种适合信息物理系统的安全架构，从底向上（从物理世界到信息世界），分别为数据接收层、网络访问层、数据管理层、智慧服务层。

信息物理系统安全架构



# 大纲

一、信息物理系统简介

二、信息物理系统安全综述

三、信息物理系统信息安全测评

# 三、信息物理系统信息安全测评

## CPS信息安全实时性测评

- CPS异常威胁实时监测
- CPS信息安全风险评估
- CPS信息安全风险预测方法

# 三、信息物理系统信息安全测评

- CPS异常威胁实时监测

## 基于特征库匹配的实时监测方法

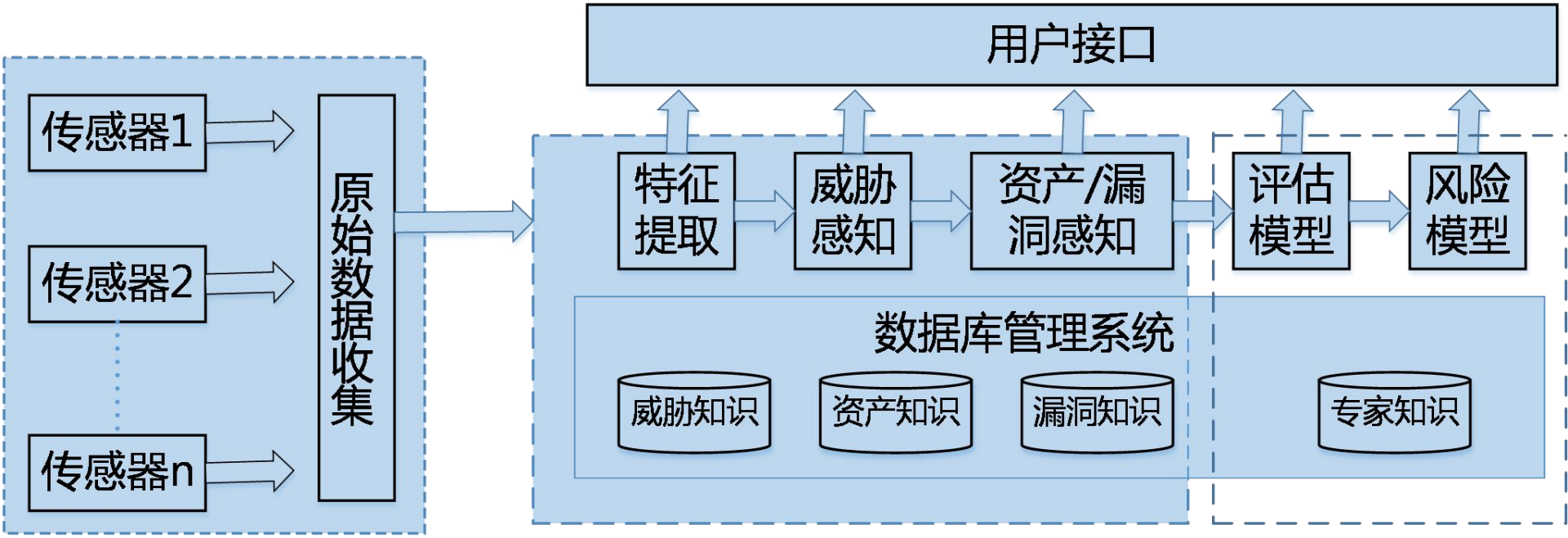
- 依赖于预先定义的异常模式数据库
- 通过比对，发现异常时报警

## 基于统计分析的实时监测方法

- 确定测量基线（确定基线、时间相关基线）
- 异常监测

# 三、信息物理系统信息安全测评

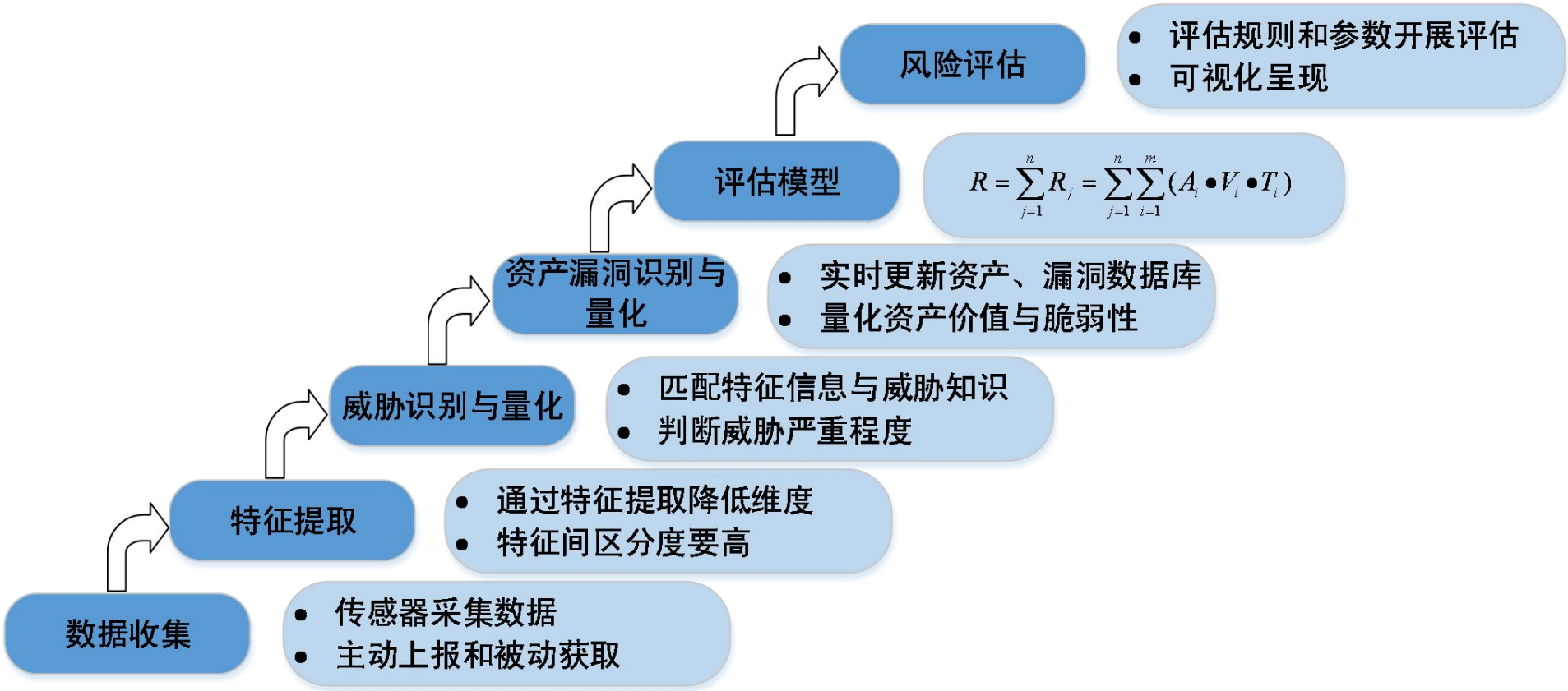
- CPS信息安全风险评估




**风险评估框架**

# 三、信息物理系统信息安全测评

## CPS风险评估流程



# 三、信息物理系统信息安全测评

## CPS风险评估模型（基于隐性马尔科夫模型的风险评估）

网络中每台主机具有N个状态： $S=\{s_1,s_2,\ldots,s_N\}$

某主机在某一时刻的状态序列： $X=\{x_1,x_2,\ldots,x_t\},x_t\in S$

主机可收到M种攻击： $V=\{v_1,v_2,\ldots,v_M\}$

攻击序列： $Y=\{y_1,y_2,\ldots,y_t\},y_t\in V$

状态转移矩阵： $P=(p_{ij})_{N\times N}\Rightarrow p_{ij}=P(x_{t+1}=s_j\mid x_t=s_i),1\le i,j\le n$

观察矩阵： $Q=(q_{ij})_{M\times N}\Rightarrow q_{ij}=P(y_t=v_i\mid x_t=s_j),1\le i\le m,1\le j\le n$

t时刻主机的总风险 $R_t=\sum_{i=1}^{N}R_t(i)=\sum_{i=1}^{N}\gamma_t(i)C(i)$

# 三、信息物理系统信息安全测评

- CPS信息安全风险预测

神经网络预测法

- 输入训练样本，自学习调整权值，运用模型开展映射
- 容错性、稳健性好，但训练时间长、可信解释困难

时间序列预测法

- 通过时间函数预测风险
- 应用方便、操作性好，但函数建模过程复杂

支持向量机

- 非线性映射到高维特征空间，进行线性回归
- 预测绝对误差小，但实时性精度有待提高

谢谢！