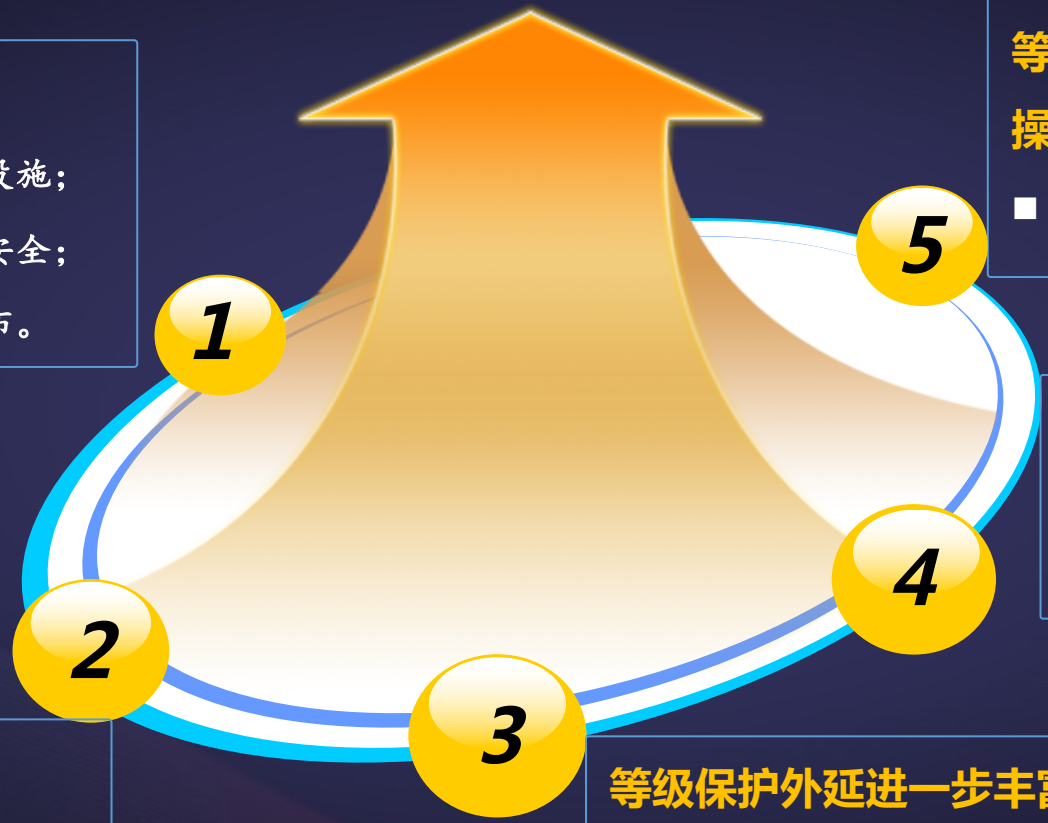
网络安全等级保护定级指南解读

李明，公安部信息安全等级保护评估中心

新形势下的等级保护制度



网络安全引起空前关注。

- 作用：辅助系统 – 支撑平台 – 基础设施；
- 关注：信息安全 – 信息保障 – 网络安全；
- 重视：《网络安全法》千呼万唤终颁布。

《网络安全法》确立制度地位。

- 21条规定：国家实行网络安全等级保护制度；
- 31条规定：关键信息基础设施在网络安全等级保护制度的基础上，实行重点 保护。

等级保护标准体系进一步提升适用性和可操作性。

- 核心标准启动修订

等级保护政策体系进一步细化和完善。

- 等级保护条例即将颁布；
- 配套管理规范启动编制。

等级保护外延进一步丰富和完善。

- 等级保护对象形态不断扩充（工业控制系统、云计算平台等）；
- 工作内容更加完善（供应链安全、通报预警等）。

- GA/T 1389-2017 《信息安全技术 网络安全等级保护定级指南》
- GA/T 1390.2-2017 《信息安全技术 网络安全等级保护基本要求 第2部分：云计算安全扩展要求》

修订

CONTENTS

信息安全技术
网络安全等级保护定级指南


信息安全技术
信息系统安全等级保护定级指南

Information security technology—
Classification guide for classified protection of information system security

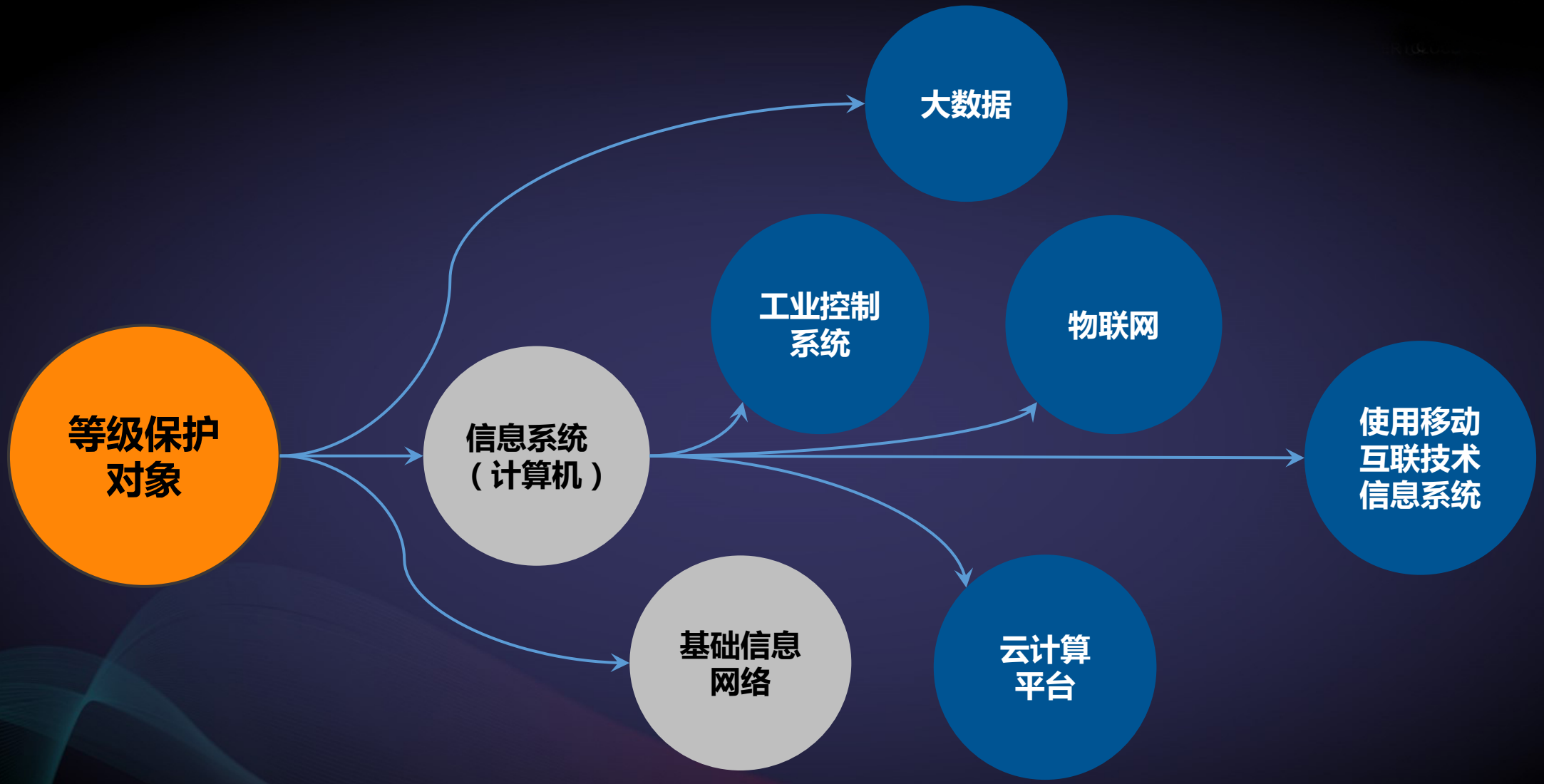
等级保护对象（修订）

网络安全等级保护工作的作用对象，主要包括基础信息网络、工业控制系统、云计算平台、物联网、使用移动互联技术的网络和大数据等。

3.1

等级保护对象　target of classified security

信息安全等级保护工作直接作用的具体的信息和信息系统。


等级保护
对象
信息系统
（计算机）
大数据
工业控制
系统
物联网
使用移动
互联技术
信息系统
基础信息
网络
云计算
平台

网络（新增）

由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。（与网络安全法保持一致）

基础信息网络（新增）

为信息流通、网络运行等起基础支撑作用的网络设备设施，包括电信网、广播电视传输网、互联网、业务专网等。

关键信息基础设施（新增）

公共通信和信息服务、能源、金融、交通、水利、公共服务和电子政务等重要行业和领域以及其他一旦遭到破坏、丧失功能或数据泄露，可能严重危害国家安全、国计民生和公共利益的网络系统。

大数据（新增）

仅在可扩展架构中才能实施存储、操作和分析，具备数量大、种类多、处理速度快和可变化等主要特性的数据集合。

大数据平台（新增）

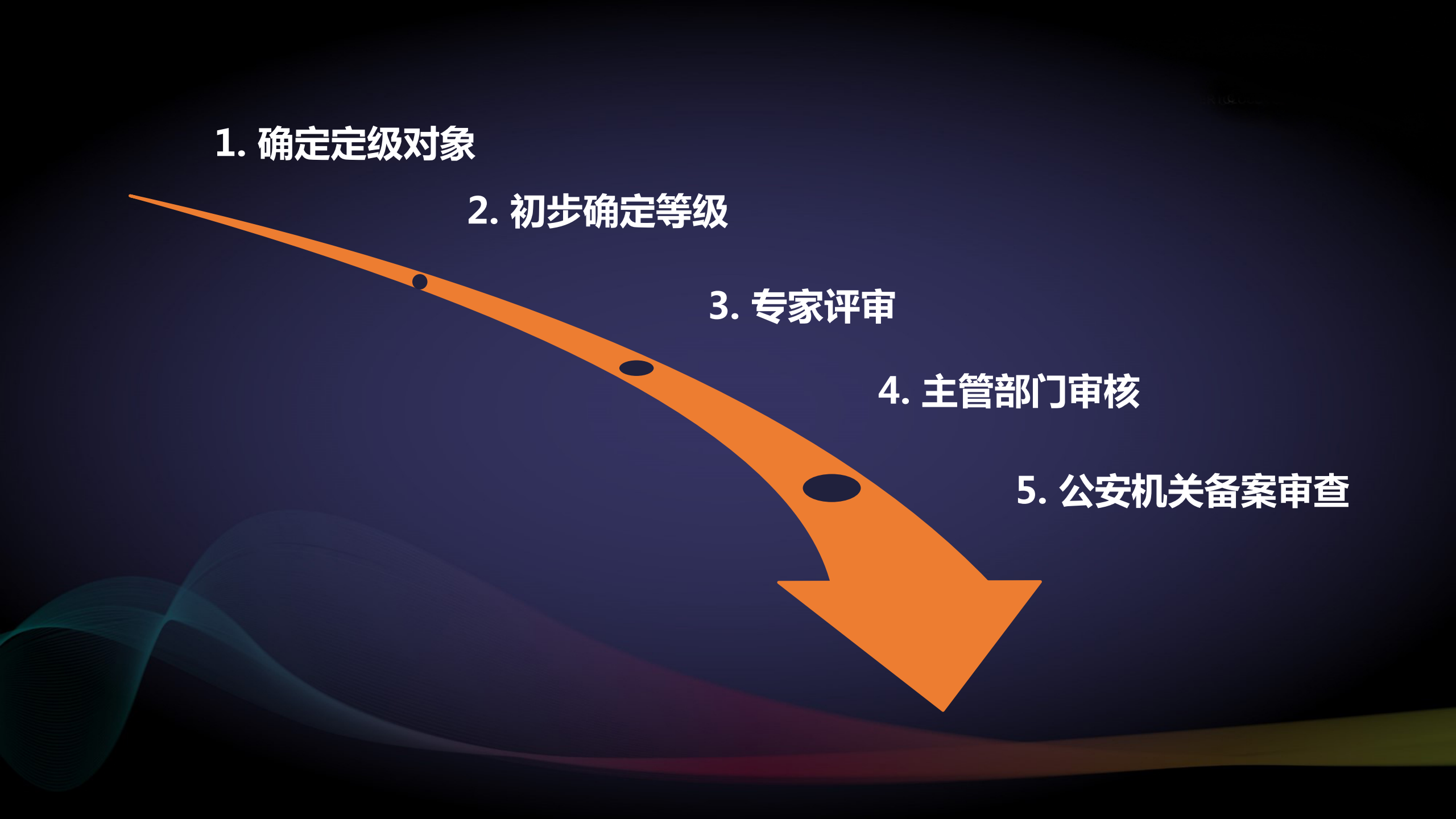
采用分布式存储和计算技术，提供大数据的访问、处理和存储，支撑大数据应用安全高效运行的软硬件集合。

第三级，等级保护对象受到破坏后，会对公民、法人和其他组织的合法权益产生特别严重损害，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

表 1　定级要素与安全保护等级的关系

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级


1. 确定定级对象
2. 初步确定等级
3. 专家评审
4. 主管部门审核
5. 公安机关备案审查

- 具有确定的安全责任主体
- 承载相对独立的业务应用
- 包含相互关联的多个网络资源

作为定级对象的信息系统应具有如下基本特征：

a) 具有唯一确定的安全责任单位。作为定级对象的信息系统应能够唯一地确定其安全责任单位。如果一个单位的某个下级单位负责信息系统安全建设、运行维护等过程的全部安全责任，则这个下级单位可以成为信息系统的安全责任单位；如果一个单位中的不同下级单位分别承担信息系统不同方面的安全责任，则该信息系统的安全责任单位应是这些下级单位共同所属的单位。

b) 具有信息系统的基本要素。作为定级对象的信息系统应该是由相关的和配套的设备、设施按照一定的应用目标和规则组合而成的有形实体。应避免将某个单一的系统组件，如服务器、终端、网络设备等作为定级对象。

c) 承载单一或相对独立的业务应用。定级对象承载“单一”的业务应用是指该业务应用的业务流程独立，且与其他业务应用没有数据交换，且独享所有信息处理设备。定级对象承载“相对独立”的业务应用是指其业务应用的主要业务流程独立，同时与其他业务应用有少量的数据交换，定级对象可能会与其他业务应用共享一些设备，尤其是网络传输设备。

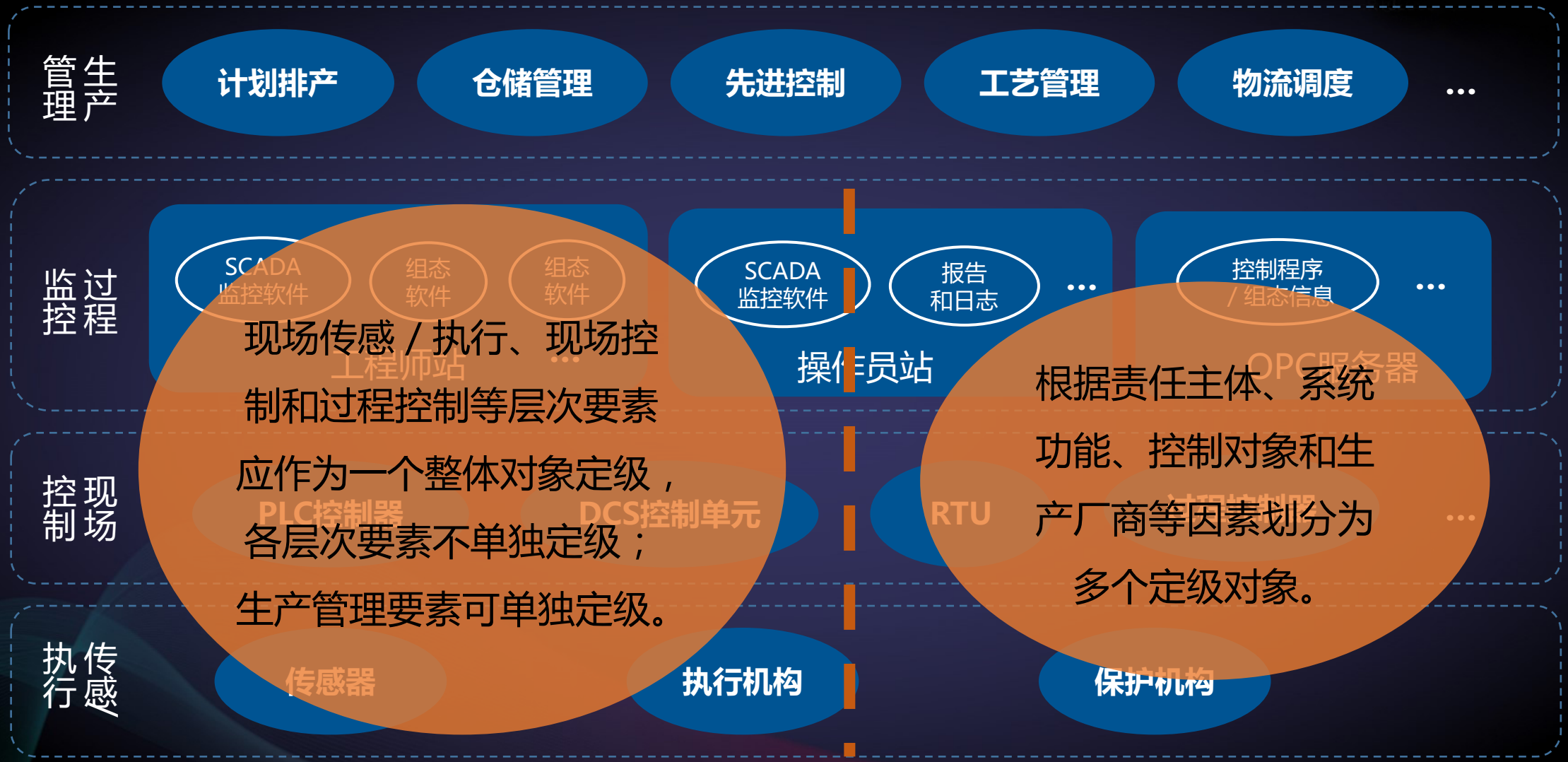
基础信息网络

对于电信网、广播电视传输网、互联网等基础信息网络，应分别依据服务类型、服务地域和安全责任主体等因素将其划分为不同的定级对象。

跨省业务专网可作为一个整体对象定级，也可以分区域划分为若干个定级对象。

现场采集/执行、现场控制和过程控制等要素应作为一个整体对象定级，各要素不单独定级；生产管理要素可单独定级。

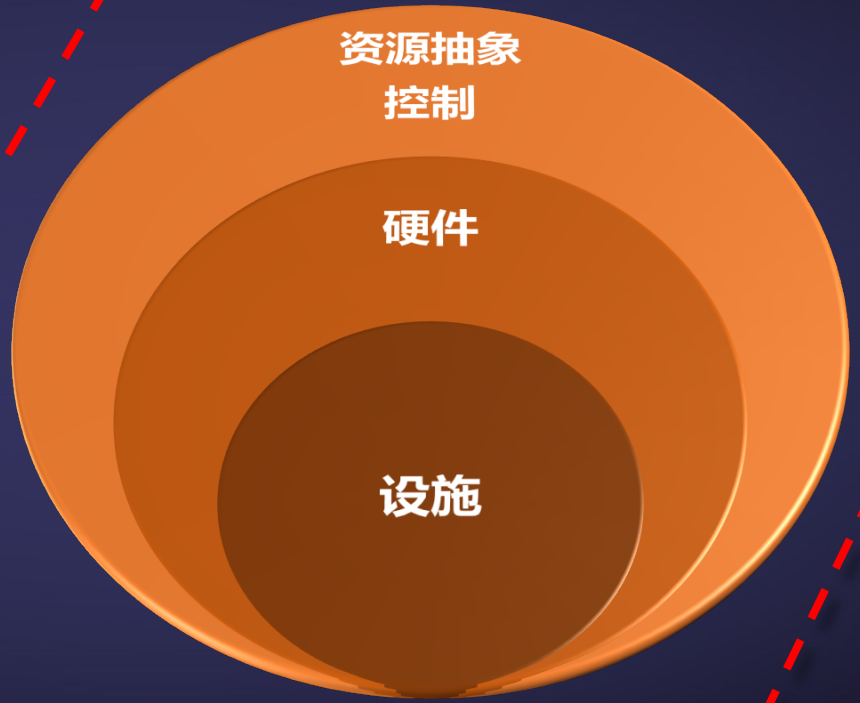
对于大型工业控制系统，可以根据系统功能、责任主体、控制对象和生产厂商等因素划分为多个定级对象。


管理 生产
计划排产
仓储管理
先进控制
工艺管理
物流调度
...
监控 过程
SCADA 监控软件
组态 软件
组态 软件
SCADA 监控软件
报告 和日志
...
控制程序 / 组态信息
...
工程师站
操作员站
OPC服务器
控制 现场
PLC控制器
DCS控制单元
RTU
...
执行 传感
传感器
执行机构
保护机构
现场传感/执行、现场控制和过程控制等层次要素应作为一个整体对象定级，各层次要素不单独定级；
生产管理要素可单独定级。
根据责任主体、系统功能、控制对象和生产厂商等因素划分为多个定级对象。

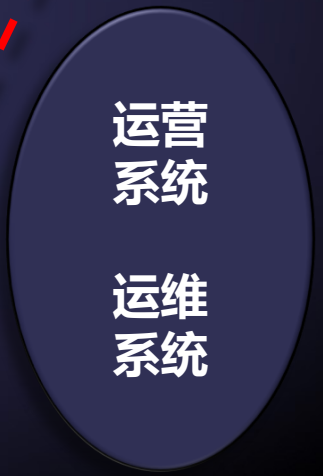
应将云服务方侧的云计算平台单独作为定级对象定级，云租户侧的等级保护对象也应作为单独的定级对象定级。

对于大型云计算平台，应将云计算基础设施和有关辅助服务系统化为不同的定级对象。

- 在云计算环境中，应将云服务方侧的云计算平台单独作为定级对象定级，云租户侧的等级保护对象也应作为单独的定级对象定级。



- 对于大型云计算平台，应将云计算基础设施和有关辅助服务系统划分为不同的定级对象。



物联网

物联网主要包括感知、网络传输和处理应用等特征要素，应将以上要素作为一个整体对象定级，各要素不单独定级。。

移动互联网

采用移动互联技术的网络主要包括移动终端、移动应用、无线网络等特征要素，应与相关有线网络业务系统作为一个整体对象定级

大数据应作为单独定级对象进行定级。

安全责任主体相同的大数据、大数据平台和应用可作为一个整体对象定级。

初步确定等级

1. 确定业务信息／系统服务受到破坏时所侵害的客体；
2. 确定对客体的侵害程度；
3. 确定安全保护等级。

对于基础信息网络、云计算平台，应根据其承载或将要承载的等级保护对象的重要程度确定其安全保护等级，原则上应不低于其承载的等级保护对象的安全保护等级。

对于大数据，应综合考虑数据规模、数据价值等因素，根据数据资源（完整性、保密性、可用性）遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的侵害程度等因素确定其安全保护等级。

THANKS

敬 请 批 评 指 正

www.cspec.org.cn