《安全工程与运营》知识点串讲

一、安全工程

（一）安全工程理论基础

1. 安全工程概念：广义的工程包括了狭义工程的范围。
2. 安全工程的原则：全生命周期的原则，同步规划、建设、使用的原则。
3. 安全工程的方面：动机、机制、策略、保证。
4. 安全工程理论基础

（1）系统工程：方法论、软科学；霍尔三维模型（**时间、知识、逻辑**）。

（2）项目管理：**有限**资源约束对**所有的工作**管理，包括**质量、进度**和**成本**管理。

（3）质量管理：以高质量的**过程控制**保证**高质量的产品和服务**（结果）。

（4）**能力成熟度**：个人及组织的过程控制质量水平的高低为 **CMM（1-5 级）**。

（二）安全工程理论模型

1. **SSE-CMM** 基础

（1）SSE-CMM 发展：美国国家**安全**局（NSA）。

（2）SSE-CMM 范围：即项目管理、质量管理、系统工程、能力成熟度等。

（3）SSE-CMM 作用：甲方-**获取方，乙方-提供方，第三方-评估方**。

2.**SSE-CMM** 的内容

2.1 域维

（1）构成：类（3 类）、**PA**（过程区域-22 个）、BP（基本实施）。

（2）内容：

— 类：**工程类**、项目类、组织类。

— 工程类：**风险过程**、**工程过程**、**保证过程**。

— 风险过程：**评估**影响、**评估**威胁、**评估**脆弱性、**评估**安全风险。

— 工程过程：**安全**需求、**安全**输入、**安全**控制、**安全**态势、**安全**协调。

— 保证过程：**核实确认**安全、建立**保证证据**。

2.2 能力维

（1）构成：能力级别、公共特征（CF）、通用实践（GP）。

（2）内容：

— 0 级：无特征。

— 1 级：基本执行。

— 2 级：规划执行、规范化执行、跟踪计划、验证计划。

— 3 级：制定标准过程、执行过程、协调安全实施。

— 4 级：制定测量标准、客观管理。

— 5 级：改进过程能力、改进组织能力。

二、运行维护

1. 漏洞管理：**有意**或者**无意**产生的缺陷，包括**技术**漏洞和**管理**漏洞。步骤：漏洞检测、漏洞评估、漏洞测试、漏洞加固、漏洞验证。
2. 补丁加固：**评估、测试、批准、部署、验证**。
3. 变更管理：**申请、审核、实施、验证**。

三、信息内容安全

1. 知识产权

1）**版权**和**著作权**的区别。

2）**数字对象标识符 DOI** 和**数字版权标识符 DCI** 的区别。

3）技术：数字水印、数字签名、收费等方式。

2. 信息保护

2.1 信息安全分类：**个人**信息、**组织**信息、**国家**信息。

2.2 网络舆情

1）网络**舆情**和舆情**事件**的区别。

2）网络舆情事件需要政府及官方媒体进行监督和引导。

四、社会工程学攻击及防护

1.社会工程学与**社会工程学攻击**的区别

2.社会工程学知识包括：心理、精神、生理、社会学、经济学、金融、法律等。

3.社会工程学攻击预防：**学习和提高认知，吸取经验和教训。**

（END）

温馨提示：为了减少学习的负担和聚焦核心，知识点总结写的是关键的精要的要点，并非是知识点的全文，请一定进一步结合官方的教材进行扩充补充、理解和掌握全面，以免产生以偏概全的问题。