湖南省第一届工业互联网安全大赛暨2024年中国工业互联网安全大赛湖南省选拔赛理论知识竞赛命题说明

为了参赛选手更有效地备赛，以及确保竞赛组织的严密性和有效性，根据湖南省第一届工业互联网安全大赛暨2024年中国工业互联网安全大赛湖南省选拔赛技术方案，对理论知识竞赛的命题工作作一个细化说明。

**一、理论知识竞赛的范围及所占总分比例**

理论知识竞赛的知识范围分6个模块，分别是：工业互联网安全政策法规，占10%；工业互联网安全标准规范，占5%；工业互联网安全理论与基础知识，占15%；工业互联网安全技术，占25%；工业互联网安全管理，占5%；工业互联网安全运行，占25%；工业互联网安全分类分级10%、工业互联网数据安全5%。

**二、试题类型和分值**

理论知识竞赛试题均为客观题，分别是：(1) 单项选择题；(2) 多项选择题。共计100道题目，题目总分300分。

**三、理论知识竞赛时间**

预赛理论知识竞赛时间为1.5小时，决赛理论知识竞赛时间为1小时。

**四、考试方式**

采用计算机考试。

**五、命题和组卷方式**

命题采用专家命题，建立具有一定规模的竞赛题库，采用按比例随机组卷的方式生成理论知识竞赛试题。

**六、复习参考书**

供参考教材清单如下:

(1)魏毅寅，柴旭东. 工业互联网：技术与实践[M].北京：电子工业出版社，第2版。

(2)威廉·斯托林斯. 网络安全基础:应用与标准[M].北京：清华大学出版社，第6版。

(3)魏强，王文海，程鹏. 工业互联网安全：架构与防御[M].北京：机械工业出版社。

(4)闫怀志. 工业互联网安全体系理论与方法[M].北京：科学出版社。

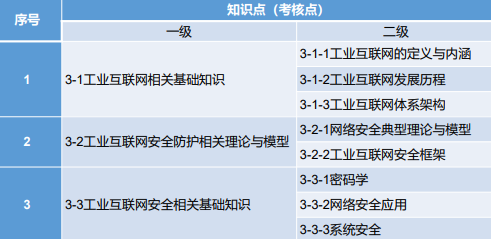
**七、每套赛卷各模块的题目类型和数量分配**

根据每套赛卷的题目的总量和各模块所占的比例，综合计算分配题目数量。

**(5)各模块知识点(考核点)命题分解——工业互联网安全政策法规模块**













湖南省第一届工业互联网安全大赛暨2024年中国工业互联网安全大赛湖南省选拔赛预赛理论知识竞赛样题

考试时间：90 分钟 考试形式：上机考试

**一、单项选择题（共60题，每题3分）**

1. 针对SCADA控制系统可能面临的攻击，可以采取的防护措施不包括？

A 限制人员操作 B 抵御完整性攻击和重放攻击

C 数据机密性保护 D抵抗中间人攻击

2. 工控系统广泛应用于电力、石化、医药、航天等领域，已经成为国家关键基础设施的重要组成部分，作为信息基础设施的基础，电力工控系统安全面临的主要威胁不包括？

A 内部人为风险 B 黑客攻击 C 设备损耗 D 病毒破坏

3. 以下哪个操作容易导致工控被病毒感染：

A 任意插入U盘等介质 B 安装杀毒软件

C 操作系统打补丁 D 删除系统多余的账号

4. 2018年《工业互联网安全框架》中指出（）是确保落实工业互联网信息安全管理，支撑工业互联网系统与服务持续运行的保障。

A应用安全 B 数据安全 C检测感知 D 处置恢复

5. 《工业控制系统信息安全行动计划（2018—2020年）》实施的主要目标包括到2020年，建成工控安全管理工作体系，全系统、全行业工控安全意识普遍增强，建成“一网一库三平台”，其中一网一库分别是指什么？

A 全国在线监测网络、应急资源库 B 应急资源网络、应急数据库

C 信息共享网络、工业数据库 D 天网、工业资源库

6. 三菱 FX2N系列最多可以支持扩展到多少个点

A 30 B 128 C 256 D 1000

7 plc是什么控制系统上发展起来的

A 电控系统 B 单机片 C 工业电脑 D 机器人

8 下列指令中哪个表示是连续执行型

A MOV（P） B MOV C PLS D PLF

9 用户程序的入口是？

A OB1 B DB1 C FB1 D FC1

10 在加计数器的设置输入S端的（），将PV端指定的预置值送入计数器值。

A 高电平 B 低电平 C 上升沿 D 下降沿

11 下列不属于PLC通信联网时用到的设备是

A RS-232或RS-422接口 B PLC专用通信模块

C 普通电线 D 双绞线．同轴电缆．光缆双绞线．同轴电缆．光缆

12 工业级模拟量,哪一种更容易受干扰．

A uA级 B mA级 C A级 D 10A级

13 触摸屏通过哪种方式与PLC交流信息？

A 通讯 B I/O信号控制 C 继电连接 D 电气连接

14 在PLC梯形图中，哪种软继电器的线圈不能出现

A 输入继电器 B 辅助继电器 C 输出继电器 D 变量存储器

15 下列输出模块可以交直流两用的是

A 光电耦合输出模块 B 继电器输出模块

C 晶体管输出模块 D 晶闸管输出模块

16 S7-300 PLC可以扩展多达（）个机架，（）个模块。

A 1，7 B 4，32 C 4，44 D 21，300

17 S7-300中央机架的6号槽的16点数字量输入/输出模块占用的字节地址为

A IB8和QB8 B IB8和QB9 C IB8和IB9 D I8和Q8

18不能以位为单位存取的存储区是

A 输入映像 B 输出映像 C 内部存储器 D 外设I/O区

19 ()是系统功能。

A FC10 B FB20 C SFC30 D SFB40

20 CPU检测到错误时，如果没有相应的错误处理OB，CPU将进入（）模式。

A 停止 B 运行 C 报警 D 中断

21 哪一种Fuzzing技术更适合工控系统？

A 基于生成的Fuzzing算法 B 基于复制的Fuzzing算法

C 基于移动的Fuzzing算法 D 基于突变的Fuzzing算法

22 WDB RPC是一个基于SUN-RPC协议的调试接口，它的服务运行在UDP协议的（）端口。

A 17175 B 17185 C 18175 D 18185

23以下不属于工控厂商的是。

A Siemens B 北京合适利 C Mo D X东方电器

24 CSPV4协议通用开放端口。

A 2405 B 20000 C 9600 D 2222

25（）是Modbus协议中的一项重要内容，几乎所有的通信都包含，这也是导致Modbus网络不安全的一个主要因素。

A 设计安全 B 功能码滥用 C 缓冲区溢出 D TCP/IP漏洞

26 DNP3的安全防护总体建议是

A 使用安全版本的DNP3 B 异常行为检测

C 安全审计 D 使用网络安全设备

27 Modbus协议易于遭受中间人攻击（MiTM），攻击类型主要包括记录和()

A 隧道攻击 B 重放攻击 C 破坏性攻击 D 处理攻击

28 针对EtherNet/IP协议的攻击方法不包括

A 身份鉴别攻击 B 中间人攻击

C 终止CPU运行攻击 D 口令暴力破解攻击

29以下应用于工控网络边界的安全产品有。

A 工控主机卫士 B 工控防火墙系统

C 工控漏洞挖掘系统 D 工控基线配置核查系统

30 ()的根本所在就是通过控制如何访问目标资源来防范资源泄露或未经授权的修改。

A 结构安全 B 设备与主机安全 C 行为安全 D 基础软硬件安全

31 关于防火墙技术说法不正确的是？

A 防火墙用于限制从另一个网络对特定网络的访问。大多数企业都使用防火墙来限制从企业网络对Internet的访问。他们还可能使用防火墙限制一个内联网段对另一个内联网段的访问。

B 防火墙设备支持和实施企业的网络安全访问策略。有组织的安全策略可以提供高层次、可接受和不可接受操作的指示，从而维持整体的边界安全性，所以防火墙技术本身也是结构安全层面最为重要的安全技术手段，是实现结构安全的基础。

C 防火墙的实现形式包括搭载防火墙软件产品的服务器或者其他特殊硬件设备，防火墙会将经过它的数据包进行分析过滤，可能丢弃、重新打包、重定向或者直接放行

D 防火墙具有定义更详细和更细粒度的安全策略的能力，从而规范哪些地址、哪些端口、哪些服务或者协议允许或者被禁止访问哪些区域，就像我们生活中的门禁和保安系统。

32工控安全威胁的最大特征是全网的()性？

A 结构安全 B 设备与主机安全 C 行为安全 D 基础软硬件安全

33 不属于工控蜜罐的核心技术的是？

A 数据捕获技术 B 数据统计技术 C 数据控制技术 D 数据分析技术

34 限制对系统或漏洞的访问的方法不包括

A 单向网关 B 电子邮件和文件的访问限制

C 物理环境的访问限制 D 用电控制

35关键信息基础设施中应用于SCADA系统的是。

A 化工 B 用电采集 C 核电 D 轨道交通

36 （）为传感器和执行器提供通信接口，与通信网络进行数据和指令交换。

A SCADA B DCS C PLC D RTU

37 SCADA系统的（）安全目标的优先级最高。

A 机密性 B 完整性 C 可用性 D 隐蔽性

38 现有的SCADA入侵检测系统绝大多数属于（）技术。

A 基于主机的异常入侵检测 B 基于主机的误用入侵检测

C 基于网络的异常入侵检测 D 基于网络的误用入侵检测

39 使用SCADA系统硬件测试平台，缺点不包括

A 不能测试特定的恶意攻击

B 搭建测试平台的成本较高

C 测试平台的扩展性较差

D 测试平台不可能像实际的SCADA平台一样在设备上完全一致

40在工业控制系统中，常见的控制器不包含？

A 可编程逻辑控制器（PLC） B 可编程自动化控制器（PAC）

C 远程终端单元（RTU） D 工业控制计算机（CPC）

**二、多项选择题（共40题，每题3分）**

1 目前工控网络中漏洞挖掘的主要困难是什么？

A 系统封闭 B 接口多样 C 通信复杂 D 奖金稀少

2 传统信息系统的漏洞挖掘方法主要分为

A 红盒方法 B 白盒方法 C 灰盒方法 D 黑盒方法

3 根据漏洞出现于工控系统组件的不同，工控安全漏洞可划分为

A 工控设备漏洞 B 工控网络协议漏洞

C 工控软件系统漏洞 D 工控安全防护设备漏洞

4 对工控系统而言，可能带来直接隐患的安全漏洞也可以分为

A SCADA系统软件漏洞 B 操作系统安全漏洞

C 网络通信协议安全漏洞 D 安全策略和管理流程漏洞

5 工控系统漏洞检测的关键技术包括

A 构建工控系统漏洞库 B 基于工业漏洞库的漏洞检测技术

C 构建传统漏洞库 D 基于传统漏洞库的漏洞检测技术

6 漏洞检测的主要方法包括

A 臆断测试 B 直接测试 C 推理测试 D 凭证测试

7 ActiveX漏洞从形成上区分为

A 内存类漏洞 B 逻辑类漏洞 C 溢出类漏洞 D 指针类漏洞

8 Codesys协议通用开放端口。

A 2405 B 1200 C 2404 D 9600

9 工业控制网络协议可以分为下面几类

A 标准通信协议比如TCP/IP协议

B 国际标准或公认的标准协议，如Modbus协议、DNP3协议、IEC系列协议等

C 只有厂商自己设备支持并提供官方协议文档，如Omron FINS协议、三菱Melsec协议等 D 只有厂商自己设备支持且官方不提供协议文档，如西门子S7协议、西门子PPI协议、GE SRTP协议等

10 DNP3通信流程分为由()发送两种模式。

A 主站发起到子站 B 主站发起到主站

C 子站发起到子站 D 子站到主站的自发响应

11 可根据哪3个基本要素的赋值，可计算安全事件造成的损失

A 资产 B 脆弱性 C 威胁 D 保障能力

12安全保护类平台如（）是最低限度的安全设备要求？

A工业防火墙 B单项隔离网关

C工业协议过滤器 D数据采集隔离平台等

13安全管理类平台如（）等，在通常情况下，区域的重要级别决定了所需的安全防护强度？

A 安全监控平台 B 安全审计平台 C IDS D 工业防火墙

14 一般防火墙提供的主要服务有

A服务控制 B方向控制 C用户控制 D行为控制

15可信网络的一般性架构主要包括？

A可信安全管理系统 B网关可信代理 C网络可信代理 D端点可信代理

16 针对工控系统风险缓解措施的考量，工控系统基于主机方面的考量因素包括

A补丁策略 B重启安排 C备份策略 D主机部署方式

17 限制对系统或漏洞的访问的方法包括

A限制权限配置 B应用程序或进程的白名单与黑名单

C工控系统网络协议监测 D堡垒主机

18 工业控制网络传输的是工业设备的“四遥信息”，“四遥”指的是

A遥测 B遥信 C遥控 D遥感

19 关于工业控制网络与传统IT信息网络的不同，下列说法正确的是

A工控系统在地域上分布广阔，其边缘部分是智能程度不高的含传感和控制功能的远动装置，而不是IT系统边缘的通用计算机，两者之间在物理安全需求上差异很大。

B工业控制网络的结构纵向高度集成，主站节点和终端节点之间是主从关系。传统IT信息网络则是扁平的对等关系，两者之间在脆弱节点分布上差异很大。

C工业控制网络传输的是工业设备的“四遥信息”，即遥测、遥信、遥控、遥调。

D工业控制网络设备部件生命周期较长，一般在15-20年，传统IT信息网络部件生命周期较短，一般在3-5年，E.工业控制网络常用的通信协议为标准通用协议，而传统IT信息网络则使用专门或者私有协议较多。

20 人机界面的特点包括

A实时性 B并发处理 C系统可裁剪 D可靠性

21 当PLC投入运行后，其工作过程一般分为

A输入采样 B用户程序执行 C输出刷新 D结果分析

22 关键信息基础设施中不属于SCADA系统典型应用行业的是。

A石油石化 B轨交 C电力调度 D化工

23 针对SCADA系统特有的安全需求和存在的脆弱性，可以实施SCADA安全防护技术包括

A 安全域划分 B 安全域边界防护

C 防火墙部署 D 专人值守

24 针对SCADA系统的特殊安全需求，常用的防火墙部署方案包括

A 办公网络与控制网络间配置单防火墙

B 办公网络和控制网络之间部署带DMZ的防火墙

C 办公网络和控制网络之间部署成对防火墙

D 办公网络和控制网络之间不部署防火墙

25 根据入侵检测分析方法的不同来分，入侵检测系统主要可以分为（）两类。

A 基于主机的入侵检测系统 B 基于网络的入侵检测系统

C 误用入侵检测系统 D 异常入侵检测系统

26 现有的工业以太网大致可以分为

A 软实时工业以太网 B 硬实时工业以太网

C 同步硬实时工业以太网 D 非实时工业以太网

27 从大体上看，工业控制网络与传统IT信息网络在有着（）主要的不同？

A 网络边缘不同 B 体系结构不同

C 传输内容不同 D 网络核心不同

28在工业控制系统中，常见的控制器有

A 可编程逻辑控制器（PLC） B 可编程自动化控制器（PAC）

C 远程终端单元（RTU） D 工业控制计算机

29 在远程测控系统中，RTU是实现远程通信的关键设备，承担着中心站和测站间信息的上传下达工作，它主要有（）功能？

A 遥测 B 遥信 C 遥控 D 遥调

30人机界面的硬件部分包含()

A 处理器单元 B 显示单元 C 输入单元 D 通信接口

**参考答案**

1. **单选题**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| A | C | A | D | A | C | A | B | A | C |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| C | A | A | A | B | B | A | D | C | A |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| D | B | D | D | B | A | B | D | B | A |
| 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| A | C | B | D | D | D | C | C | A | D |

1. **多选题**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| ABC | BCD | ABCD | ABCD | AB | BCD | BC | AB | ABCD | AD |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| ABD | ABCD | ABC | ABCD | ABCD | ABCD | ABCD | ABCD | ABCD | ABCD |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| ABC | ACD | ABC | ABC | CD | ABCD | ABC | ABC | ABCD | ABCD |