HUAYI 华谊集团

网络安全相关制度培训

制造和数字化中心

2021年10月26日

主要内容：

- 信息系统上线安全规范（2020年）
- 工业控制系统网络安全管理办法
- 华谊集团私有云平台管理办法
- 华谊集团数据安全管理规范

一、信息系统上线安全规范

项目管理及计划阶段：

- 确定信息系统的安全保护等级，明确信息系统所对应的公司内部系统级别；
- 系统测试计划中应包含安全性测试
- 在信息系统项目建设各重要阶段（项目计划、需求、设计、测试及试运行）应填写《上线技术规范落实情况表》

信息系统分级原则：

为规范建设标准，合理分配资源，优化运维力量，集团对信息系统进行分级管理，按信息系统划分的等级，分配不同的资源，制定不同的安全策略、防护措施和保障手段。

系统等级判定标准分为三个指标：

- 实时性要求高
- 对生产经营影响程度大
- 可能造成的损失大

信息系统分为三个级别：核心系统、重要系统、一般系统。其中同时满足以上三个指标的为核心系统；满足以上三个指标之一的为重要系统；不满足以上三个指标的为一般系统。

需求分析阶段：

- 整体需求中应该包含关键的安全功能需求
- 操作系统、数据库版本的选择应符合本规范要求
- 应该包含系统连续性功能需求
- 应该包含系统运维监控功能需求

设计阶段：

- 根据确定的需求分析书设计系统安全、连续性、运维监控设计方案

测试阶段：

- 应在甲方提供的测试环境中进行测试
- 项目组需要在测试环境中完成相关运维、监控环节的测试，完善运维手册、用户手册、监控手册、应急手册等；
- 确保所有设计的安全功能均能得到落实和实现；
- 测试环境操作系统、中间件、应用程序、数据库均不应存在可被跨网段利用的高危漏洞

试运行阶段：

- 系统试运行前应提交系统测试报告、用户手册、运维手册、监控手册、应急手册、交付清单等；
- 完成连续性测试；
- 如有与其他系统共用的情况，有与其他系统关联的情况的，由运维人员根据相关情况，及时修正运作流程和应急指引；
- 如发现由于应用系统缺陷造成有直接操作后台数据、非应用系统界面操作等非规范运维操作的，应及时整改；
- 由于应用系统缺陷，造成系统主要功能无法实现，业务无法保障，应及时退出试运行阶段，重回测试阶段

二、工业控制系统网络安全管理办法

工业控制系统网络安全管理办法

工业控制系统主要由过程监控、现场控制和网络三部分设备及部署在这些设备上的软件组成

（1）过程监控设备包括各类服务器、工程师站、操作员站、OPC站、APC站等。

（2）现场控制设备包括控制站、通信站和远程单元等。

（3）网络设备包括路由器、交换机、网关、有线或无线远程调制解调器等。

基本原则

（一）工业控制系统实行全生命周期管理，安全防护设施建设应坚持**同步设计、同步施工和同步投用**的原则。

（二）工控网络安全管理基本原则：“谁主管谁负责、谁使用谁负责、谁运维谁负责”。

总体要求

- 逐步建立和完善工业控制系统的网络安全加固和建设模版；
- 定期对工业控制系统网络进行安全风险评估；
- 用于工业控制系统安全防护的硬件和软件产品应经过充分验证；
- 最小化系统安全原则；
- 加强工业控制系统安全防护重要性宣传。

机构及职责

集团制造和数字化中心负责集团工业控制系统网络安全总体工作，主要职责为：

- 制定并发布工控网络安全相关制度；
- 制定并发布集团工控安全标准建设模版，对各企业工控安全工作开展检查指导；
- 定期组织企业开展工控安全培训，培育工控安全队伍；
- 对外部服务商资质、工控安全入围产品、工控安全落地方案进行审查。

机构及职责

各工业生产企业主要职责：

- 指定工控网络安全分管领导和责任部门，建议由负责自控仪表的部门负责本企业工业控制系统的安全防护工作；
- 根据集团制度制定各单位实施细则，加强工控系统日常安全管理；
- 严格按照集团标准建设模版，落实系统安全技术方案，组织部署工业控制系统的安全防护措施。

机构及职责

集团成立网络安全运营团队，在集团制造和数字化中心指导下，开展工控安全技术支持工作，主要职责为：

- 联合外部专业力量，协助各公司处置工控安全应急事件；
- 按集团要求，对各生产企业工控安全运行情况进行检查；
- 按集团要求，组织各生产企业开展工控安全应急演练。

一 安全软件选择和管理

- 在过程监控设备和工业主机上应采用经过离线环境中充分验证测试的防病毒软件或应用程序白名单软件，只允许经过企业授权和安全评估的软件运行，防止病毒或未经企业授权的程序运行。
- 应建立防病毒和恶意软件管理机制，对工业控制系统及临时接入的设备（调试用便携式计算机、移动存储设备等）采取病毒查杀等安全预防措施。
- 防病毒软件宜采取离线升级的方式更新病毒库。

二 配置和补丁管理

- 做好工业控制网络、工业主机和工业控制设备的安全配置，建立工业控制系统配置清单，定期进行配置审计。
- 对重大配置变更制定变更计划并进行影响分析，配置变更实施前进行严格安全测试。
- 企业应加强工业控制系统软件补丁的管理，补丁升级在线下模拟系统中进行验证，在不影响系统可用性、实时行和稳定性的前提下实施更新。

三 边界安全防护

- 明确工业控制系统的防护边界，采用工业防火墙在工业控制系统内部边界进行横向防护，采用网闸等网络单向隔离设备在工业控制系统与企业信息网络之间进行纵向隔离。
- 禁止没有采取防护措施的工业控制网络与外部网络连接。
- 工业控制系统网络边界防护策略采用白名单机制，安全最小化配置允许规则，保证网络通信。
- 工业防火墙、网闸等网络隔离设备应具备检测结果报警及报警远传功能，具备工控环境适用能力。

四 物理和环境安全防护

- 对工程师站、操作站、服务器、控制器等核心工业控制系统软硬件所在区域采取访问控制、视频监控、专人值守等物理安全防护措施。
- 系统控制柜机房出入口应采取书面登记方式，有条件的增加门禁，鉴别和记录进入的人员。
- 对进入机柜间作业的外来人员应建立审批流程，并安排专人陪同，限制和监控其活动范围。
- 应拆除或封闭过程监控设备和工业控制设备上不必要的USB、光驱、无线接口等，在工业控制设备上使用移动介质时应采取专盘、专用、专人管理等手段，实施严格访问控制。

五 身份认证

- 应在工业控制系统过程监控设备的登录、应用服务资源访问等过程中适用身份认证管理。
- 应合理分类设置账户权限，以最小特权原则分配账户权限。
- 建立并完善工业控制系统和相关工业通信设备等的登录账户及密码管理机制，明确规定密码强度、有效期等工作要求，密码长度不少于8位，至少包含大、小写字母、数字、特殊字符中的三种。

六 远程访问安全

- 原则禁止工业控制系统面向其他网络开通HTTP、FTP、Telent等高风险通用网络服务。
- 原则上禁止通过远程访问方式操作工业控制系统。
- 保留并定期备份工业控制系统的相关访问日志，对操作过程进行安全审计。通过审计账户登录、访问时间、操作内容等日志信息，追踪并定位非授权的访问行为。

七 安全监测和应急预案演练

- 应在工业控制网络设置网络安全监测设备，及时发现、报告并处理网络攻击或异常行为。监测行为应不影响工业控制系统原有正常应用功能。
- 企业应制定工控安全事件应急预案，当遭受安全威胁导致工业控制系统出现异常或故障时，应立即采取紧急防护措施，防止事态扩大，并第一时间上报集团制造和数字化中心。
- 企业应定期组织工业控制系统操作、维护、管理等相关单位人员开展工控安全事件应急预案演练。

八 资产安全

- 应建立工业控制系统资产清单，明确资产责任部门。
- 建立资产使用、处置规则。
- 控制器设备每一次的配置变更，需要进行记录，不进行组态变更的时候，应及时在控制器的硬件上切换到只读模式，防止程序被恶意下载。

九 数据安全

- 对静态存储和动态传输过程中的重要工业数据进行保护，重要工业数据应加密存储，并设置访问权限。
- 定期备份关键业务数据。
- 设备生命周期结束时，应开展剩余信息保护，清除退役组件上的信息。

十 供应链安全管理

- 选择工业控制系统规划、设计、建设、运维、评估等服务商时，应优先考虑具备工控安全防护经验的单位，以合同等方式明确服务商应承担的信息安全责任和义务。
- 应和外部服务单位签订保密协议，防范敏感信息外泄。
- 在服务商进行现场调试时，要求服务商将手机锁在手机柜里，如需短距离对话，使用对讲机进行，防止手机私拉热点以及手机拍照。

十一 事故事件管理与处置

- 各公司一旦发生工控安全事件，应在事件发生三十分钟内上报集团制造和数字化中心，并按照应急预案开展先期处置。信息公司工控安全专业团队应积极协助企业开展工控安全事件处置。
- 工控安全事件引起生产事故的，按照集团《生产安全事故及责任追究管理规定》执行。

三、华谊集团私有云平台管理办法

资源管理

- 私有云在“资源需求和建设、资源评估、资源分配、资源回收和调整”等方面存在三个主要主体责任方：私有云综合管理部门、私有云维护部门、业务需求部门。

资源管理

- 华谊集团制造和数字化中心为私有云“私有云综合管理部门”，具有以下职责：
- 负责定期征集各“业务需求部门”IT系统资源需求，结合私有云运行情况，开展私有云资源池的建设、扩容，牵头组织完成立项、设计和工程建设相关工作；
- 参与审核各“业务需求部门”的系统设计方案，评估方案和资源需求类型、数额及资源投入预算的合理性。
- 审批各“业务需求部门”提出的私有云资源申请需求。

资源管理

- “业务需求部门”为私有云资源使用单位。
- 负责根据自身业务需求进行系统立项，按照分布式架构规划上层应用软件，根据私有云架构组织制定业务设计方案；
- 负责组织包括私有云综合管理部门、私有云维护部门、设计单位、集成商等相关单位进行设计方案会审，与各部门就项目资源分配达成一致方案；
- 负责在业务部署上线后，维护业务操作系统及其之上的应用软件，保障私有云监控代理软件的运行状态，配合“私有云维护部门”根据业务系统实际资源利用率情况对资源占用进行调整和优化；
- 负责所申请的主机资源的操作系统及业务应用的安全管理，配合安全检查，并对不符合要求的主机或应用系统进行整改；
- 集团总部各部门及各子公司等私有云资源使用单位为“业务需求部门”。

资源申请和需求评估

- 业务需求部门申请分配私有云资源，需同时具备两个前提条件：（1）该系统属于当期私有云综合管理部门参与项目方案会审的项目。（2）该系统的IT资源需求在私有云当期私有云综合管理部门的需求调查阶段已经申报并作为当期私有云建设依据。
- “业务需求部门”向私有云维护部门进行私有云资源申请，由“私有云维护部门”进行初审后交“私有云综合管理部门”审批，申请材料中需包含立项批复文件、项目设计方案、资源申请等内容。

资源分配和业务上线

- 资源配置完成以后，“业务需求部门”项目负责人牵头项目集成商，完成系统的部署和测试。
- 业务系统正式上线前，集团网络安全运营团队、“私有云综合管理部门”、“私有云维护部门”应与“业务需求部门”通过召开业务上线沟通会等形式，就接口人、基础配置信息进行核对和交接，明确维护分工界面以及责任和权利，确保各项支撑工作高效开展；集团网络安全运营团队应根据管理规定，对业务系统安全加固、漏洞扫描、Agent安装、接入等执行情况进行审查，明确系统符合入网条件后业务需求部门方可启动业务上线。

资源运行评估及调整回收

- “业务需求部门”结合业务系统运行情况可以提出资源变更申请，“私有云综合管理部门”评估系统资源利用率情况和私有云资源余量，审核通过后由“私有云维护部门”予以实施。
- 业务系统因业务量萎缩、退网或调整等原因造成资源闲置，应由“私有云综合管理部门”与“业务需求部门”共同协商启动资源回收流程。
- 业务系统下线后要求执行“资源回收，再分配”过程。“业务需求部门”不能将下线的主机等资源直接划拨其他业务系统使用，应保证业务系统与资源数据对应关系的准确性。

四、华谊集团数据安全管理规范

数据采集安全

- 遵循数据最小化原则
- 数据提供部门（责任部门）应对采集的数据进行分级分类标识

数据传输安全

- 主要包括物理传输安全和通信传输安全
- 物理传输过程中应确保移动介质安全和传输人员操作安全
- 通信传输过程中应确保传输设备安全和网络安全
- 涉及到单位敏感信息和个人隐私信息的数据传输场景，应在数据分级分类的基础上进行加密传输或专线

数据存储安全

- 不同类别和级别的数据分开存储
- 建立数据存储冗余策略和管理制度，以及数据备份与恢复操作过程规范。
- 确保在人为破坏、软硬件故障、灾难灾害或突发公共安全事件等情况下，避免数据的丢失和损坏

数据处理安全

- 建立数据脱敏规范和流程
- 严格规范员工个人生物识别信息应用

个人敏感数据脱敏规则：

- 【身份证号】显示最后四位，其他隐藏。共计18位或者15位，比如：**********1234。
- 【固定电话】 显示后四位，其他隐藏，比如：*******3241。
- 【手机号码】前三位，后四位，其他隐藏，比如：135****6810。
- 【地址】只显示到地区，不显示详细地址，比如：上海徐汇区漕河泾开发区***。
- 【电子邮箱】 邮箱前缀仅显示第一个字母，前缀其他隐藏，用星号代替，@及后面的地址显示，比如：d**@126.com。
- 【银行账户】前六位，后四位，其他用星号隐藏每位1个星号，比如：6222600**********1234。

项目类敏感数据脱敏规则：

- 【项目名称】：前6个字加星号显示；
- 【客户名称】：前6个字加星号显示；
- 【地址】：同“个人敏感数据脱敏规则”中的地址脱敏规则；
- 【银行账户】：同“个人敏感数据脱敏规则”中的银行账户脱敏规则。

数据交换安全

- 按分级分类的标准，制定不同的审批权限清单

	A类	B类	C类
内部共享	经过需求部门和数据责任部门的上级领导审核；存在风险不确时，需请示公司总裁级领导审批	经过需求部门和数据责任部门的领导通过	经数据责任部门领导审批
外部共享	需请示公司总裁级领导审批	报分管领导进行评估审核	经数据责任部门分管领导审批

数据销毁安全

- 彻底删除，并无法复原

谢谢 Thank you