南京郵電大學
Nanjing University of Posts and Telecommunications

边端设备检测及近场通信安全仿真平台

目录

01 项目背景——漏洞数量及等级分布

图 1 近十年漏洞数量走势图(数据来自于 CNVD)

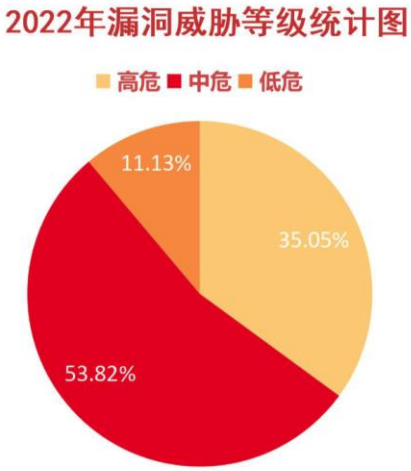


图2 2022 年收录漏洞按威胁级别统计(数据来自于 CNVD)

图1 ：近十年来，CNVD 披露的漏洞数量呈现上升趋势。尤其是在 2018 年至 2021 年之间，漏洞数量大幅增加。然而，2022 年的数据显示漏洞数量有所下降。反映了近一年时间来，对漏洞的产生采取了有效的措施，但由于网络安全威胁的持续存在，仍然有必要继续加强网络安全防护。

图2 ：可以看出大多数漏洞为中高危。这意味着如果这些漏洞被利用，可能会对网络造成严重的损害。因此要重视漏洞管理工作，并加强对中高危漏洞的修补和防护。同时，这也需要注意资产的安全性，虽然低危漏洞只有 11.13% ，但如果这些资产很重要或者被大量使用，仍然有可能带来潜在的风险

01 项目背景——漏洞原因及威胁分析

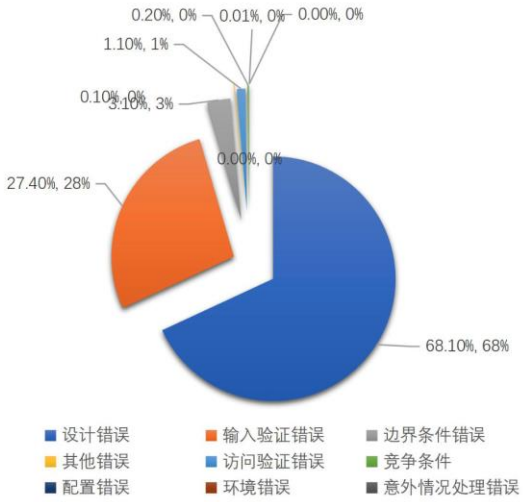


图1 2022 年漏洞产生原因统计(数据来自于 CNVD)

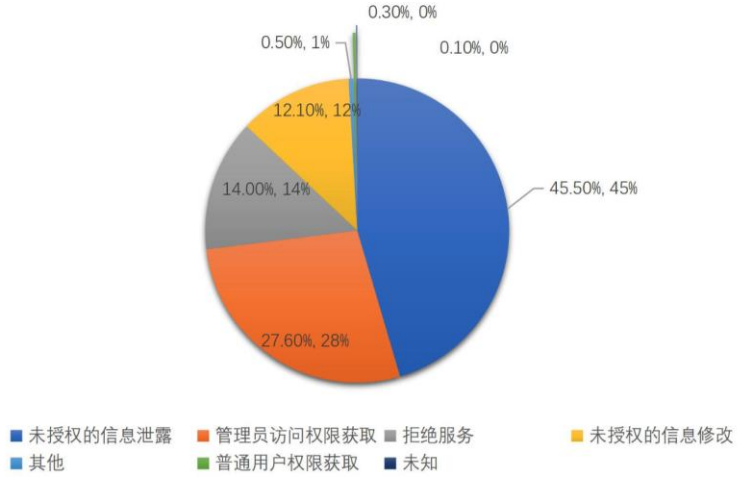


图2 2022 年漏洞引发威胁统计(数据来自于 CNVD)

图1 ：设计错误以及输入验证错误是漏洞产生的主要原因，这些漏洞的存在，可能会导致恶意用户注入恶意数据破坏系统安全获取敏感信息，因此在做漏洞检测以及安全防御时，因重点针对这两类错误去进行设计，同时，也应注意系统的访问验证、竞争、配置和环境的安全性评估，以确保系统的安全性。

图2 ：未授权的信息泄露是导致威胁的主要原因，数据即生命，数据泄露可能会对电力系统造成无法估量的损失，保护信息安全是非常重要的。因此，采取有效的防御手段以及安全认证机制是保护信息不受泄露的重要手段。

01 项目背景——电力系统典型事件

典型事件

- 2014年，研究人员破解了西班牙电力公司智能电表采用的AES-128对称加密算法，通过向电表注入恶意代码，实现了对电表标识码篡改、修改电量读书进行窃电，甚至以此为跳板攻击其他电表，切断供电，造成事故
- 2015 年 12 月 23 日，乌克兰国家电网系统遭到黑客攻击，首都基辅部 分地区和乌克兰西部突遭大面积停电
- 2016 年 12 月 17 日，乌克兰国家电力部门再次遭遇黑客攻击
- 2019 年 3 月 7 日晚，委内瑞拉发生全国范围的大规模停电，全国 23 个州 中有 18 个州电力供应中断，这导致委内瑞拉大面积停电

事件分析

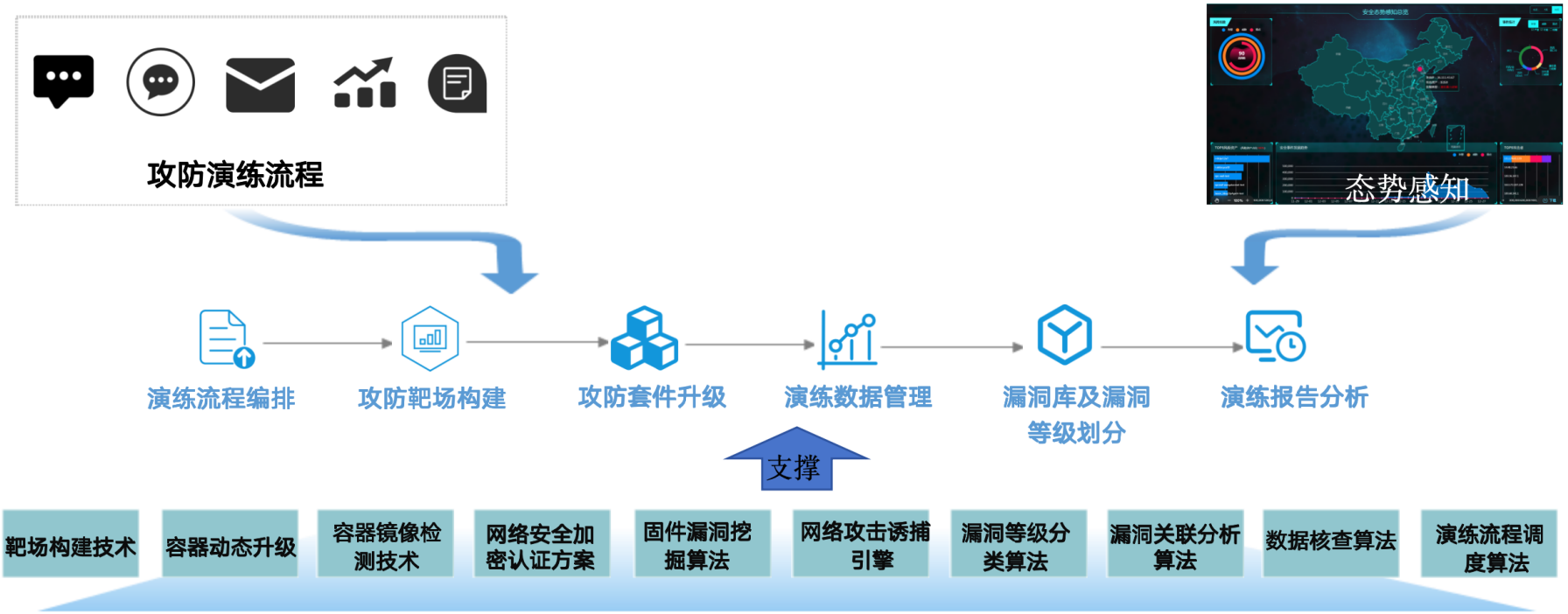
- 上述事件均为黑客直接利用电力系统漏洞或将某边端设备作为跳板对电力系统进行攻击从而达到攻击整个电力系统的目的，其具有攻击手段多样、攻击目标随机、攻击威胁巨大的特点

应对措施

- 通过构建边端设备及通信网络一体化安全仿真平台，验证固件漏洞挖掘算法的有效性，身份认证及网络防御算法的准确性等，为电力业务安全防护引擎做相关准入的有效验证。

目录

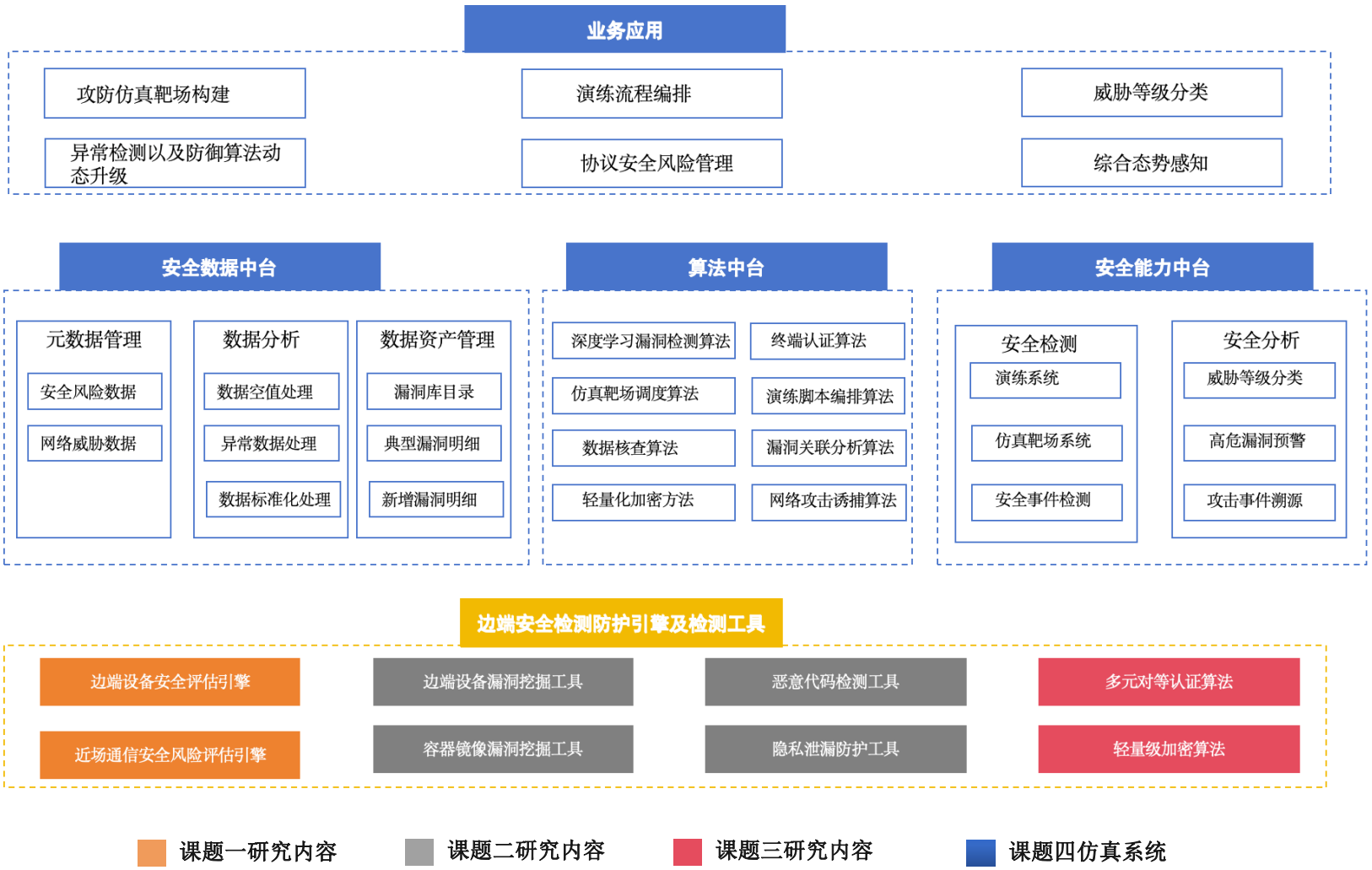
02 整体方案——总体建设目标



边端设备检测及近场通信安全仿真平台

以容器化技术、漏洞挖掘、网络加密、数据分析算法为基础，构建边端设备检测及近场通信安全仿真平台，形成攻防流程编排、攻防靶场构建、攻击防守容器动态升级、攻防动态可视化的攻防安全仿真系统，并通过综合态势感知，直观可见电力系统设备漏洞情况、网络攻防数据、全网运行态势，为电力设备及网络安全运行提供准入保障。

02 整体方案——系统架构


业务应用
攻防仿真靶场构建
演练流程编排
威胁等级分类
异常检测以及防御算法动态升级
协议安全风险管理
综合态势感知
安全数据中台
元数据管理
安全风险数据
网络威胁数据
数据分析
数据空值处理
异常数据处理
数据标准化处理
数据资产管理
漏洞库目录
典型漏洞明细
新增漏洞明细
算法中台
深度学习漏洞检测算法
终端认证算法
仿真靶场调度算法
演练脚本编排算法
数据核查算法
漏洞关联分析算法
轻量化加密方法
网络攻击诱捕算法
安全能力中台
安全检测
演练系统
仿真靶场系统
安全事件检测
安全分析
威胁等级分类
高危漏洞预警
攻击事件溯源
边端安全检测防护引擎及检测工具
边端设备安全评估引擎
边端设备漏洞挖掘工具
恶意代码检测工具
多元对等认证算法
近场通信安全风险评估引擎
容器镜像漏洞挖掘工具
隐私泄漏防护工具
轻量级加密算法
课题一研究内容
课题二研究内容
课题三研究内容
课题四仿真系统

02 整体方案——系统功能结构

02 整体方案——系统建设原则

基于标准技术规范

- 统一建设、管理与应用体系
- 统一技术规范
- 统一模型设计
- 平台功能规范要求

开放原则

- 借鉴互联网思维，提供标准化环境，实现应用与平台分离，强调开放、协作、共赢，打造开放的“生态”。

先进原则

- 引入先进技术及经验，加强自身对技术掌控能力，建设“低成本、高效率、可管理维护”的边端设备与网络安全检测平台。

安全保密原则

- 确保数据安全，防止数据泄露
- 保护自然人、法人信息安全
- 保护隐私

利旧原则

- 充分借鉴现有系统在数据、架构、应用、运维和人员等方面的储备和积累，尽量利旧现有资源。

渐进原则

- 按照“统一规划、分步实施”要求，逐步推进完善系统建设，构建试点应用。

可靠原则

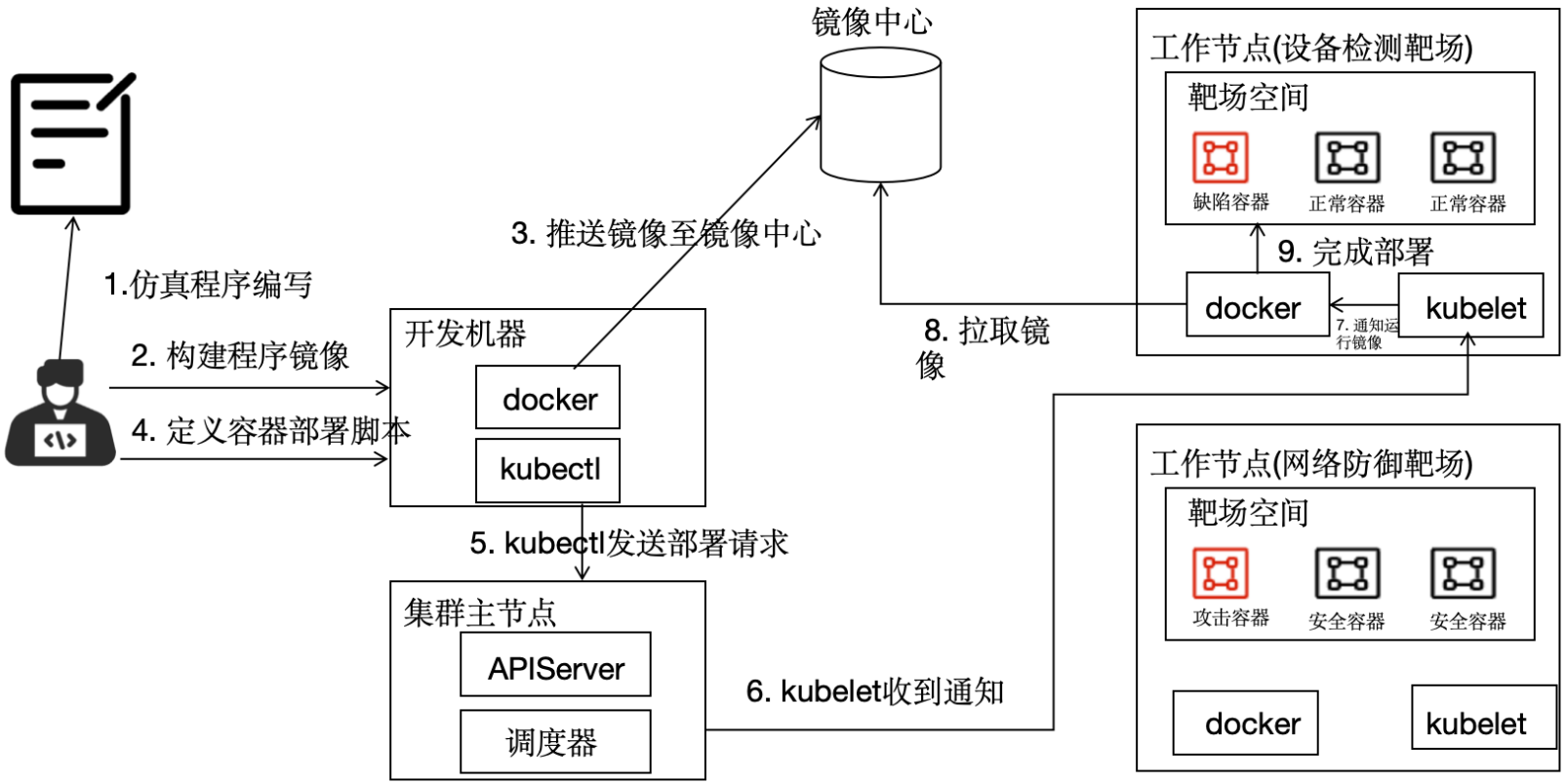
- 在技术服务和维护响应上，同用户积极配合,保证数据完整可靠。

实用原则

- 操作简单、快捷,紧密结合业务；
- 满足规范要求的效率与响应时间，操作便捷灵活。

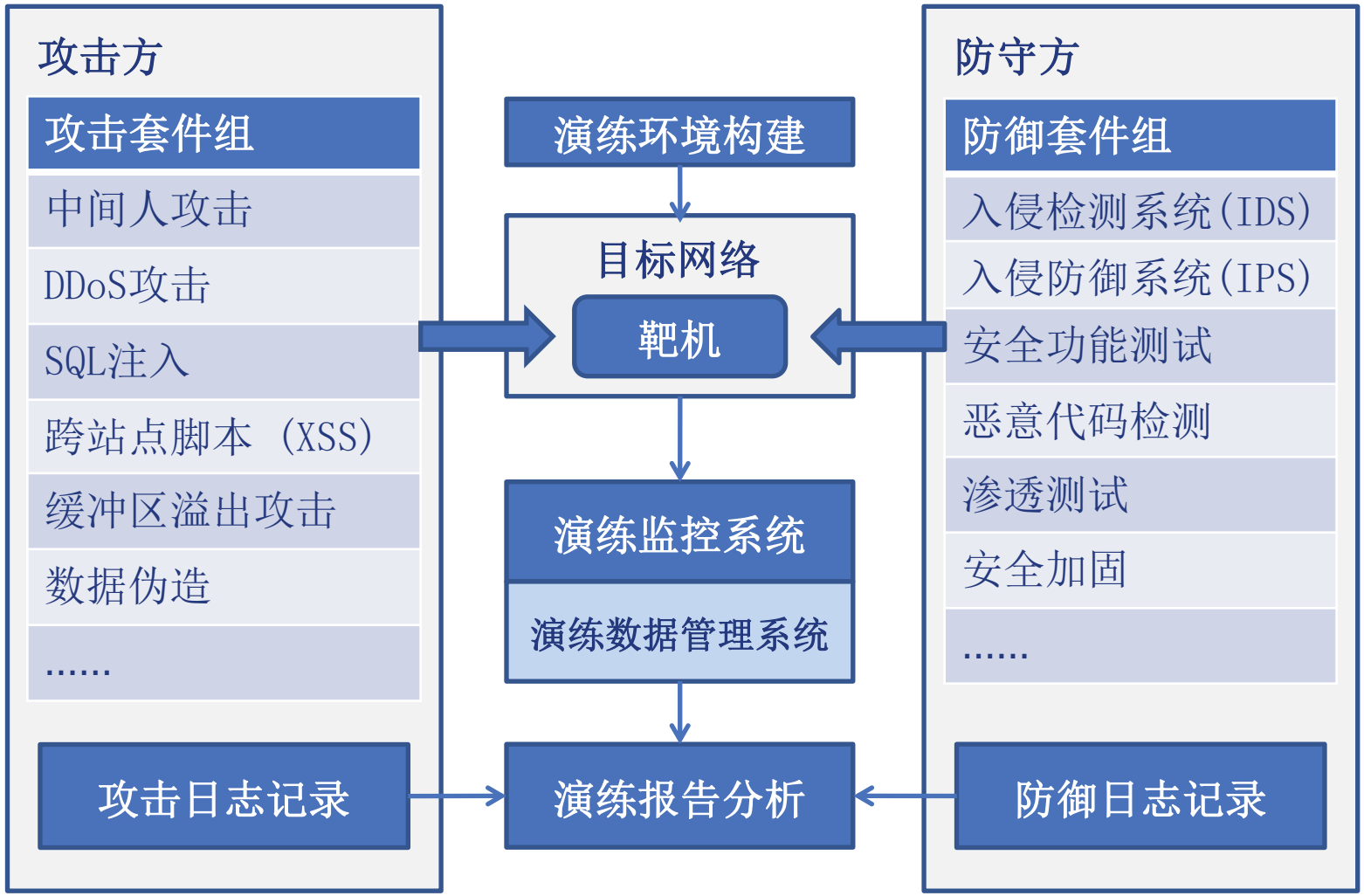
目录

03 关键技术——仿真靶场构建

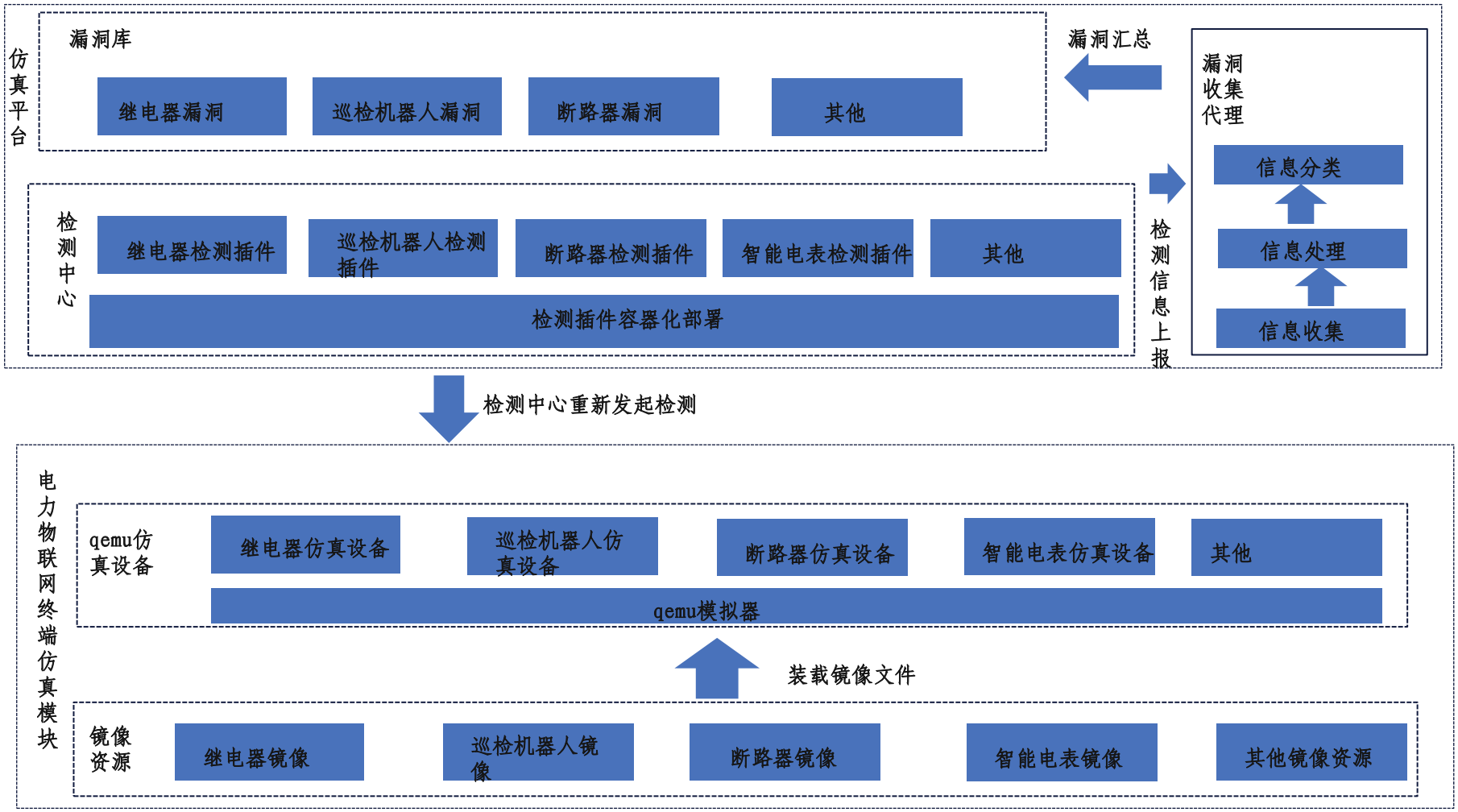


将**电力系统中的防护工具及安全检测算法编译构建成镜像**，通过容器化技术将检测算法调度到指定的靶场空间完成部署，设计**演练流程对目标靶机进行攻击，检测算法进行防御，以此为基础构建仿真靶场，达到验证检测算法是否有效的目的，为检测算法入网前的有效验证提供安全有效的检测机制**。

03 关键技术——攻防演练仿真



03 关键技术——设备漏洞仿真挖掘



03 关键技术——漏洞等级与网络安全等级评估

评分方式	名称	是否利于紧急消控	是否有较好的操作性	是否适于工程化
传统漏洞评分方式	CVSS	否	是	是
漏洞优先级技术（VPT）	SSVC	是	否	否
	MVSS	是	是	是

对环境指标项目评价值$K'_{i,j}$归一化处理，得到权重$V_{i,j}$

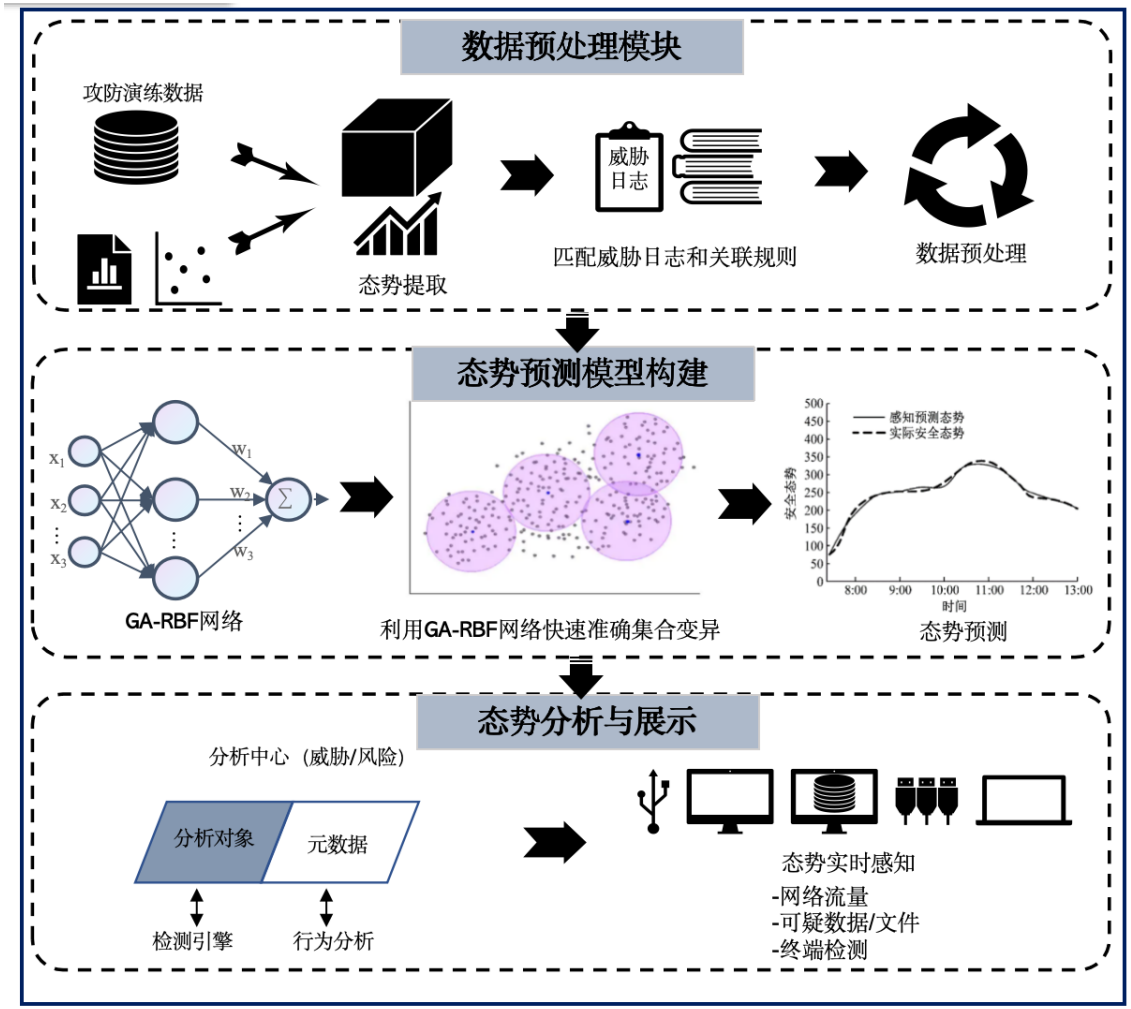
$$V_{i,j} = \frac{K'_{i,j}}{\sum_{j=1}^{|Y|} K'_{i,j}}$$

计算得出漏洞危害销控优先级排序指数V_j

$$V_j = \sum_{i=1}^{|X|} W_i \times V_{i,j}$$

注:
1. SSVC:卡耐基梅隆大学提出的特定于利益相关者的漏洞分类方法采用决策树的形式给出漏洞消控紧急程度建议。
2. MVSS:多因素漏洞评价方法(杨一未提出)，基于信息资产上的漏洞危害消控排序，与已有的研究比较更能满足实践要求

03 关键技术——综合态势感知



态势感知模型

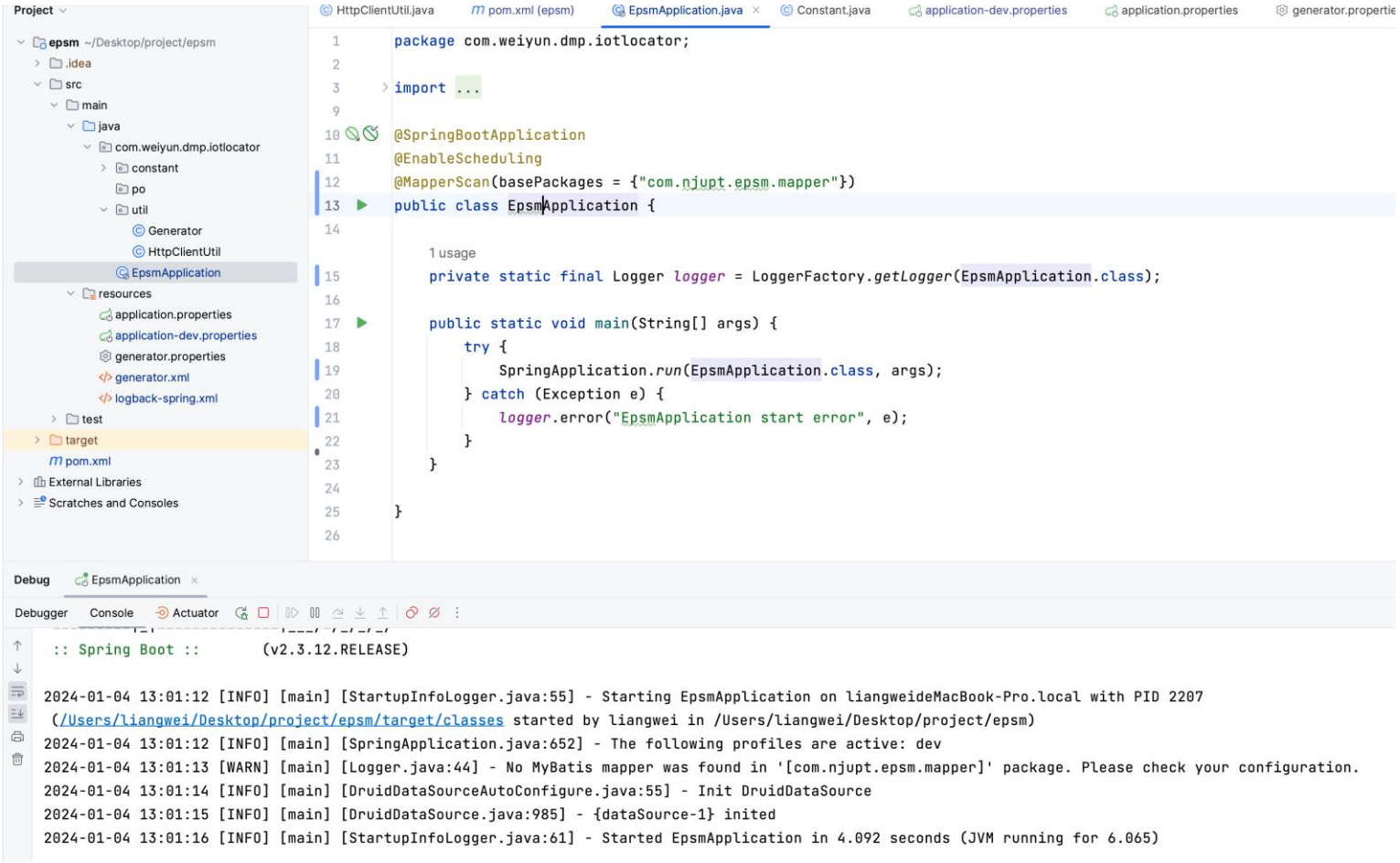
通过结合态势感知模块**对电力业务态势进行分析和解释**，有效地挖掘攻击场景并完成态势理解,通过态势感知界面进行综合展示，通过**一图可总揽电力系统整体运行情况、固件漏洞情况、网络风险及防御情况**等。

安全态势感知界面

目录

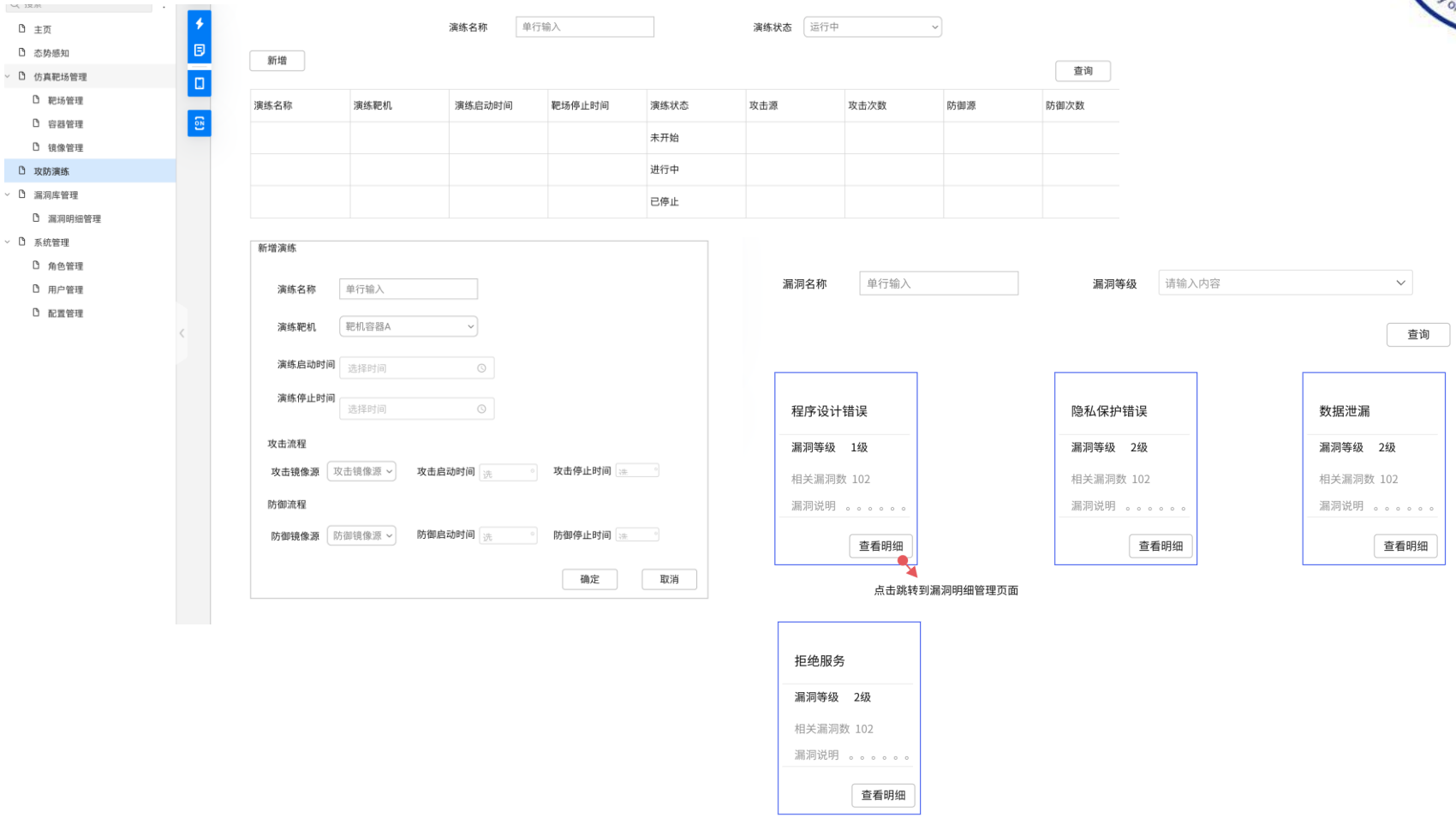
进展一：已完成开发框架构建

完成后端开发框架搭建



进展二：已完成数据库设计

进展三：已完成原型系统设计



Thank You !

欢迎大家提出宝贵意见！