**InSPUR 浪潮**  
http://www.inspur.com

**玩转开源 UBML，与你共成长**  
闫舒  
2024年10月

**01. 背景介绍**

国家、部委、山东省的发展规划均鼓励通过开源社区进行创新和发展。

* 《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》支持数字技术开源社区等创新联合体发展，完善开源知识产权和法律体系，鼓励企业开放软件源代码、硬件设计和应用服务。
* 工信部《“十四五”软件和信息技术服务业发展规划》提出培育壮大市场主体，加快繁荣开源生态，提高产业集聚水平，形成多元、开放、共赢、可持续的产业生态。计划建设2-3个有国际影响力的开源社区，培育超过10个优质开源项目。
* 《山东省“十四五”数字强省建设规划》鼓励软件开源项目建设，加强公共服务平台建设，打造软件适配平台、试验测试环境等公共服务，着力构建开源开放的技术创新和应用生态。

**“模块及组件”**

“积木”概念：通过拖拽，将模块按照自定义需求拖放到可视化的界面。

**02. inBuilder 低代码开发平台**

使用可视化页面建模工具，轻而易举搭建应用。

* 表单驱动开发，所见即所得创建应用。
* 业务专家可拖拽前端组件搭建应用页面，布局模式灵活，满足业务场景多样化需求。
* 可视化配置界面规则，满足个性化控制界面需求。
* 内置人员、组织等业务组件，快速添加标准化组件。
* 一键添加附件组件，支持在线预览Office文档。

**丰富的产品特性**

* 可视化响应式界面设计器，支持极大、大、中、小四种屏幕尺寸，自适应屏幕尺寸自动布局，满足不同尺寸屏幕显示效果。
* 支持批量调整宽度比例，拖拽调整显示顺序，滑动鼠标可视化调整宽度比例，实时预览布局效果。

**03. UBML 开源项目**

**UBML 核心特性与技术优势**

* 开发语言无关性
* 开放性：模型的标准与实现解耦，模型类型可按需求持续扩展。
* 云原生：基于微服务架构设计，支持容器化，工程化工具支持DevOps。
* 全栈模型刻画：模型数量40+，涵盖UI、API、Service、流程、领域服务、持久化等。
* 运行态定制：采用代码生成+动态解析，Hybrid模式，运行态仍可进行个性化定制。
* 模型工程化：提供工程化的结构，可与工程化工具集成，将模型视为源码。

**inIoT 社区版的物联网应用创新挑战赛**

基于UBML开源内核的浪潮海岳物联网平台inIoT，以“广泛连接、实时计算、数实融合、工业智能”四大特性，深耕行业应用场景。该平台广泛应用于国内大型企业，支持快速打造数据智能创新应用，支撑了智能制造、智慧粮食与仓储、智慧水务、智慧矿山等一系列智慧化的行业解决方案。本赛项希望通过开源社区群智创新，聚焦垂直行业领域场景，扩展行业标准协议适配，贡献具有行业特色的物联网创新应用，扩大工业软件生态范围，促进物联技术普惠发展。

**UBML 标准**

* 模型基础结构
* 经营管理类
* CAD：研发设计类
* PLC：工业控制类
* 数据采集类
* SDK：扩展机制
* 支持Angular、Vue、Java、Python等开发框架

**基于UBML开源内核的inBuilder低代码平台社区版**

支持零代码、低代码、硬编码开发全场景应用。通过inIoT物联网平台计算处理后的设备数据，可直接用于inBuilder低代码平台快速开发物联特色的创新应用。

**参赛队伍基于inBuilder低代码平台**

将物联接入的设备及计算处理后的数据，开发成具有行业特色的创新应用，如能源管理监测、智慧工地、智慧交通、安全生产、智能家居等领域。

**基于日志和大语言模型，实现智能运维**

利用大模型算法分析来自各种运维工具和设备的大量数据，自动实时检测和响应系统问题，从而提高IT运维的能力和自动化水平。提供系统日志、异常标签和API，通过包括但不限于RAG、CoT等方式，分析异常原因。

**UBML 开源项目 - 开源大事记**

* UBML项目拥有25个主要代码仓库，上线Farris Vue项目，获得Gitee推荐项目。
* 发布inBuilder社区版，正式启动社区运营。
* 关注度387，Star 751个，社区成员90人，提交数量2732次。
* 在中国程序员节获得“软件行业活跃开源社区”及“软件行业创新开源项目”奖项。

**第二个讲座：网络安全态势及攻防技术交流**

**一、什么是网络/信息安全？**

1. **什么是网络安全**

网络安全主要关注保护网络和网络设备的安全性，包括计算机网络、无线网络和网络通信。其目标是防止未经授权的访问、滥用、破坏或修改网络资源。

* **网络设备安全**：如路由器、防火墙、交换机等设备的安全配置和保护。
* **数据传输安全**：使用加密协议（如SSL/TLS）保护数据在网络上传输的安全性。
* **防御机制**：包括入侵检测系统（IDS）、入侵防御系统（IPS）等，用于检测和防止网络攻击。

**网络安全带来的影响**

网络安全已成为当今任何行业不可或缺的组成部分，无论是国家、企业还是个人，都深受其影响。从手机和电脑、邮箱、常登陆的论坛，到公司的业务系统，甚至是汽车、无人机、卫星系统，网络安全无处不在。

**近年来数据泄露事件**

* 2016年4月，济南20万名婴幼儿信息被打包出售。
* 2016年8月，国内某高校学生个人信息泄露，导致高考录取新生徐玉玉被骗。
* 2017年10月，网易用户数据库疑似泄露，影响过亿邮箱用户。
* 2017年另一事件，京东数据包泄露，包含数千万条用户敏感信息。
* 2017年1月，新浪微博超过5.38亿用户的个人信息被公开销售。
* 2020年3月，淘宝近12亿条用户数据泄露。
* 2021年6月，45亿国内快递信息遭泄露。
* 2023年2月，华住酒店数据泄露，包含2.4亿条酒店入住记录。
* 2023年8月，多家公司数据泄露，包括四通、顺丰、前程无忧等。

（注：以上事件仅为示例，具体数据和影响可能有所不同）

**四、国外网络安全现状**

1. **在“卡脖子”安全技术中**

有效维护网络主权是攻防对抗的重要目标，是战略性安全问题。国际社会对网络主权概念颇具争议，但以美国为首的西方国家已在政策、组织和技术等先发优势基础上建立了维护网络主权和霸权的能力。例如，2010年美国成立专门的网络司令部，并构建了大量网络武器库。域名解析系统作为支撑网络运行的核心部件，被美国牢牢掌握，由于其管理和运营结构是中心化的，这也使其成为制裁他国的利器。如2012年叙利亚“断网”事件就显示了这一点。

1. **车联网安全方面**

国际上对车联网的生命周期要求、软件平台规范、软件代码级规范、数据安全规范等均有明确的标准和要求。美国橡树岭国家实验室、俄亥俄州立大学等均设置专门实验室研究车内安全、联网安全、数据安全及车联网安全的评测平台。

1. **专业大型靶场方面**

网络安全基础研究平台由美国、欧洲最先进行研究。目前各国致力于研究大型虚实结合网络靶场，将物联网、工控等难以虚拟化的系统接入虚拟靶场，进行关键场景攻防测试。美国已具备国家网络（NCR）、物联网、电力等多个专用靶场，可以将异构异域靶场互联互通。

**发展趋势**

1. **零信任安全模型**

* **概念**：基于“永不信任，总是验证”的原则，假设内部和外部网络都不可信。无论用户在何处访问资源，都需进行身份验证和授权。
* **主要技术**：身份和访问管理（IAM）、多因素认证（MFA）、微分段等。
* **作用**：提高安全性，降低数据泄露和攻击风险。通过实时监控和动态访问控制，及时响应潜在威胁。

1. **供应链安全**

* **概念**：关注保护供应链中所有参与方的安全，防止由于第三方的漏洞导致的攻击。
* **主要技术**：风险评估工具、持续监控等。
* **作用**：降低由于供应链漏洞导致的安全事件，增强整体安全态势。

**前沿技术**

* **深度学习与行为分析**：利用深度学习算法分析用户和设备行为，以发现潜在的安全威胁。通过训练数据识别正常行为模式，并检测异常活动，提高安全检测的准确性和效率。

**几个名词**

* **黑客**：对计算机科学、编程和设计方面具有高度理解的人。除了精通编程和操作系统的人外，对硬件设备创新的工程师通常也被认为是黑客。现在精通网络入侵的人也被看作是黑客。
* **黑客精神与黑客文化**：崇拜技术、追求创新的精神与文化。推动自由软件运动，发现漏洞并协助管理员修补它。
* **脚本小子**：利用他人所撰写的程序发起网络攻击的网络闹事者。通常不懂得攻击对象的设计和攻击程序的原理。
* **弱口令**：强度不够，容易被猜解的口令（密码）。
* **Webshell**：以asp、php、jsp或cgi等网页文件形式存在的一种命令执行环境，黑客常用其控制网站服务器。
* **注入点**：可以实行注入的地方，通常是一个访问数据库的连接。
* **上传点**：网站中可以上传文件或图片的URL，黑客可能利用这些上传点的漏洞把可执行脚本上传至目标服务器。

**如何成为专家**

* **考证**：国内如软考、华为系、公安部系、信息安全测评中心系等认证；国际如ISC的CISSP、CCSP等认证。

（注：以上认证和名词仅为示例，具体可能有所不同）