**基于工作流引擎的管理项目**

**介绍:**

企业，组织甚至个人不时的面对不同的项目根据Badiru [Bad88]，项目是一组有组织的活动，以实现一组既定目标。它通常有明确的起点和终点，明确的预算、资源的参与，明确的完成标准，并且必须是非常规的。

一些项目在组成上可能具有相似的“外观”，其他项目的外观可能不同但结构相似，还有一些项目在所有方面都完全不同。不同的业务部门往往有不同的项目，但某个公司可能会反复面对同一类型的项目。

现有不同类型的现有软件来支持项目管理，从基于PC到基于大型机，从通用到特定问题，每个软件都有自己的优点和缺点。现有系统支持各种功能的组合，但支持主要与项目的规划阶段有关，在项目的监测和控制领域以及支持不同支持组之间的通信联系和信息流。

工作流是信息系统中基于网络的新兴技术。工作流系统旨在通过利用资源需求和工作项流的组织知识的集合来帮助人们执行工作程序。声称工作流非常强大，可以指定，执行，监视和协调分布式环境中的工作项流。因此，选择工作流技术来支持项目管理的通信，监视和控制功能。

所提出的系统建立在强大的内部模块化结构上以存储基本的项目的属性，使外部部分尽可能灵活，便于其适应每种应用中的特殊特征。内部结构对用户是透明的，并赋予系统灵活性使系统不仅限于一种特殊的项目：

* 灵活性使系统不仅限于一种特殊的项目;
* 模块化使类似的项目可以从过去的经验中共享经过验证的模块，而不是从头开始；
* 项目管理软件提供的项目计划功能与基于工作流技术的系统提供的跟踪，通信和控制功能的互连。

系统的外部部分将是用户友好的，易于使用，易学易用的。

**工作流引擎组件：**

为了提供一个共同的基础，我们将介绍工作流的基本要素和构建块。这些构建块是用作最低层次结构中工作流系统控制的基本组件。

**A)流程：**

流程是为满足特定目标而执行的一系列活动。该流程可以是部门，跨部门或跨组织的内部流程。根据工作的性质，流程可以从非常简单的任务到非常复杂的任务。在项目管理术语中，过程类似于任务。例如：SelectMaterials，ObtainMaterials和Experiment是MSP示例中的一些过程。

**B)活动：**

活动是可由单个角色或资源管理或执行的最小工作单元。实现活动本身将导致达到上层的下一层次的目标，当然也是最高层次的主要目标。该定义类似于项目管理中的活动定义。例如：ChooseMaterials和Approval of selected materials是MSP示例中任务SelectMaterials下的一些活动。

**C)角色：**

角色是具有一些共同特征的一组资源，其中一个可以替换另一个。定义角色的主要目标是增加流程的灵活性，并最大限度地减少因人员频繁更改或不可用而导致的延迟。在项目管理中，角色在资源中表示，并且通常按特征，功能，资格或组织进行分组。这些组对应于一个角色。例如：化学高级工程师是MSP示例中的一个角色。

**D)演员：**

演员或玩家是可以扮演工作流系统角色的特定人，软件或设备。 actor有一个标识，它可以执行的角色列表，以及定义其特征的各种属性。在项目管理中，参与者或参与者对应于各个资源。例如：Tom和Jerry是MSP示例中化学高级工程师角色的演员。

**E) 路由：**

路由是流程的流程表示。它描述了与活动相关的某些对象（如文档和表单）的运动路径。该路由仅显示活动之间的优先级以及角色和活动之间的关系。更详细的路线控制将由规则定义。在项目管理中，路径对应于项目的网络图。

**F) 规则：**

规则或脚本用于实现Route。该规则是一种系统语言，它定义了与工作流相关的以下元素：

●how - 对象的路由方式（串行，并行）

●when - 路由将被触发的时间或持续时间

●what - 路由的对象类型

●whose - 路由对象的源

●who - 路由对象的目标。

该规则类似于项目管理网络流量条件，但工作流程中的规则可以提供更详细的控制。

**工作流模型**

**介绍：**

本节中讨论的大多数工作都集中在工作流执行的授权模型或安全约束处理上。工作流授权模型（WAM）12,13,55）（Atluri＆Huang 96，Atluri，Huang Bertino 97）概念和执行模型，集中于任务依赖和事务处理中授权的执行通过使用Petri网（PN）。工作流设计器在工作流的构建时间期间使用授权模板（AT）定义授权的静态参数。当任务开始执行时，AT用于派生实际授权。在多级安全（MLS）工作流环境中，任务被分配到不同的安全级别。此外，WAM通过提出安全Petri网（SPN）来扩展PN模型，该安全Petri网用于检测和防止所有违反安全性的任务依赖性。虽然WAM讨论了授权流与工作流的同步以及静态方法中时间约束的规范，但仅支持工作流安全性是不够的。这是因为工作流需要更多的动态方法来在工作流执行期间同步授权流。例如，将根据任务执行期间生成的事件向代理授予/撤消特权。WAM只关注任务状态和原语中的授权，而不是资源访问中的授权。此外，WAM不讨论任务中同一对象内的操作流程的顺序。在工作流中，我们需要在不同方面（如任务，事件和资源）调查授权流。此外，我们还需要从代理方面考虑授权流程，而不仅仅是工作流中任务之间的相互依赖性。 WAM仅讨论授权库（AB）以存储在工作流执行期间授予的所有权限，但它不考虑代理和任务方面的历史概念。 WAM处理Authorization的安全属性，MLS在任务依赖项中处理Integrity的安全属性，但他们不处理可用性和职责分离的安全属性。

我们将通过下一章中的几个工作流示例演示WAM的局限性。基于工作流授权模型（WAM），在[27]中提出了一个名为Secureflow的基于Web的WFMS，Secureflow使用简单的4 GL语言，如SQL，指定授权约束主要用于职责分离尽管Secureflow支持角色分配的安全约束，但它对于工作流安全性来说还不够，因为工作流安全性需要支持从构建工作流到工作流运行时的不同安全约束。 Secure low处理授权和职责分离的安全属性，但它不处理Integrity和Availability的安全属性。

基于任务的授权（TBA）[52,53]（Thomas＆Sandhu 93,94）如图3.2所示，提供了一个概念模型来描述信息系统中任务授权的建模和管理。 TBA描述了抽象和组合，依赖关系，控件的合并，委派和撤销，授权到期和截止日期，死锁授权，失败和异常处理等问题。尽管TBA在概念工作流模型中呈现任务依赖性和任务授权中的事务控制表达式，但它不足以支持工作流安全性这是因为TBA只关注工作流中任务和代理之间的分配，但工作流安全性要求任务代理和资源之间的分配。TBA处理Integrity和Sep aration of Duties的安全属性，但它不处理授权和可用性的安全属性。

服务拒绝服务模型[43]（Millen 92）如图3.2所示，提供了资源分配和销毁的概念模型。拒绝服务保护库（DPB）已被定性为靠近可信计算机基站（TCB）的资源监视器。虽然DPB支持进程的等待时间策略，但仅支持工作流安全性是不够的。这是因为该模型不讨论工作流级别中角色和任务的资源管理，该模型仅讨论操作系统级别的资源管理

我们已经实施了一个名为CAPBASED-AMS Capability and Event-driven Activity Management System的研究原型WFMS。CAPBASED AMS基于18中提出的协作式问题解决（CPS）的集中式架构，但CPS不会调查CPS环境中的安全问题。在图3）所示的38]（Hung，Karlapalem＆Gray 98）中，我们通过列举最小特权，文档访问的动态授权和文档推导的问题，为活动执行期间文档安全性执行中的不同问题提出概念模式。来自事件观察的特权信息。

在（37（图3中显示的Hung和Karlapalem 97）中，我们介绍了CAPBASED-AMS的基本逻辑和执行模型，并提出了一种以任务为中心的安全执行方法，其中检查安全约束并允许任务只有在没有违反任何安全约束的情况下才能执行。上述工作有助于进一步开展[33,31] [图3所示的[Hung＆Karlapalem 97]]中提出的CapBasED-AM系统的工作，其主要贡献是整合为安全活动执行开发逻辑和执行框架的安全要求和处理机制。我们通过考虑系统基础设施，安全要求下的匹配，安全策略和可信PSA来提供CapBasED-AMS。

**总结：**

通常，所有相关工作都没有详细考虑任务语义和任务强加的安全要求。任务语义包括从工作流中的任务协调，执行任务的代理，所需资源以及执行任务所涉及的约束中获得的方面。历史（审计跟踪）是检测安全威胁（如感兴趣的焦点（COI））的重要概念。此外，在工作流执行期间任务，代理和资源之间的授权流程也是工作流安全性中的重要主题。安全工作流模型必须能够确保完整性、可用性、以及可用性和职责分离的安全属性。基于安全工作流模型，我们将工作流安全性扩展到最小特权安全性的概念，其中每个代理被授予在会话中执行分配的任务所需的最严格的特权集（或最低间隙）。安全风险因子（SRF）用于衡量与执行一组相互依赖的任务的一组代理相关联的风险级别。根据主题具有低SRF和高故障恢复能力的功能选择将任务分配给代理的方法。

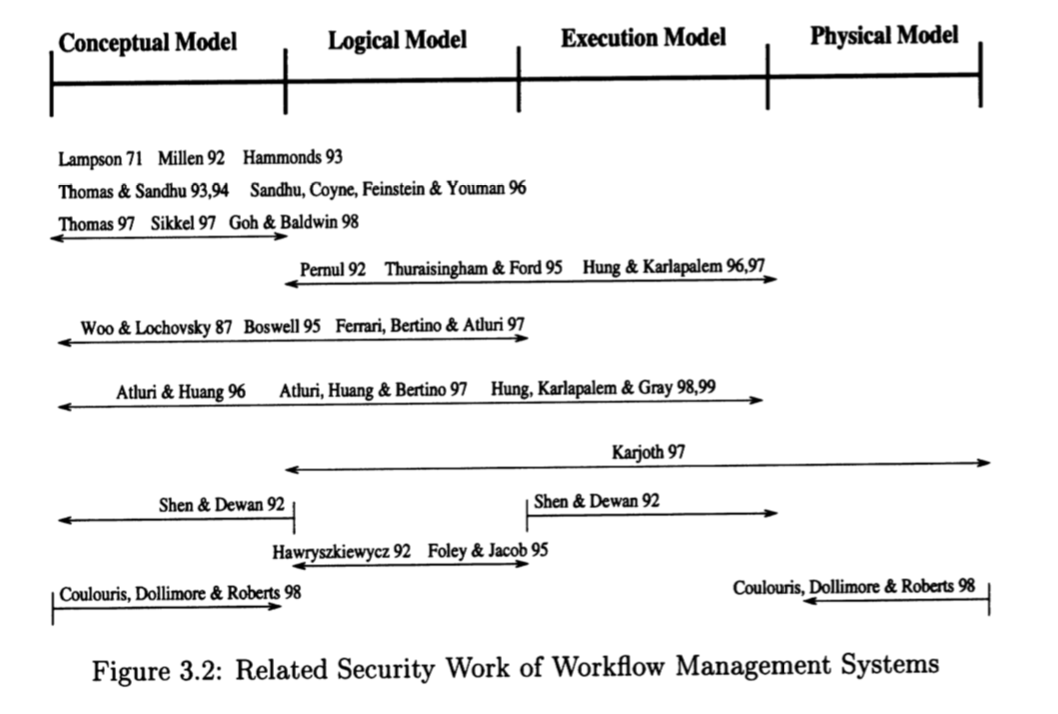


图 3-2