论信息系统的安全风险评估

摘要：

2005 年 3 月，我参加了某石化公司的实验室信息管理系统项目的开发工作，该系统作为该石化公司产品质量信息管理平台，将实验室的自动化分析仪器与计算机网络进行联结，实现自动采集样品分析数据，对样品检验过程、实验室资源进行严格管理，实现从原料进厂、生产、中间控制直至成品出厂的全过程质量数据管理，以及全公司范围内质量数据的快速传递与共享。我作为项目负责人，负责项目实施中的项目管理工作和系统投运后的运行维护工作。

为了做好系统的开发和应用，必须对系统将面临的安全风险进行评估。我在系统的安全风险评估方面采取了如下措施：分析现有业务流程和新系统信息流的安全因素，做好安全风险分析；建立安全风险评估标准，对安全风险评估分级、分类；在信息系统的各个阶段，反复对安全风险进行评估。系统在 12 月底通过验收，在两年多的运行期间，没有发生重大安全问题，系统建设、运行中的安全风险评估起了很大作用。

正文：

2005 年 3 月，我参加了某石化公司的实验室信息管理系统(以下简称 LIMS，Laboratory Information Management System）项目的开发工作， LIMS 主要实现四个方面的功能：实验室数据管理；实验室资源管理；实验室自动化仪器联结；检验数据 WEB 发布。LIMS 项目实施完成后，LIMS 将作为该石化公司产品质量信息管理平台，通过 LIMS 将实验室的自动化分析仪器与计算机网络进行联结，实现自动采集样品分析数据，按照 ISO/IEC 17025 实验室管理体系对样品检验过程、实验室资源进行严格管理，实现从原料进厂、生产、中间控制直至成品出厂的全过程质量数据管理，以及全公司范围内质量数据的快速传递与共享。

我从系统的可行性分析阶段就参与系统的调研工作，项目立项后作为 LIMS 项目的项目负责人，主要负责项目管理，同时负责项目的需求分析、系统集成、系统测试和系统投运后的运行维护工作。

系统拟采用 C/S 和 B/S 混合架构方式，后台数据库采用 Oracle 9i，前端客户端采用 Visual C++6.0 开发，WEB 端采用 ASP.NET 技术开发，B/S 和 C/S 模式均要支持三层结构。

不仅要从开发技术上要保证系统的信息安全，也要从管理上预知系统开发过程和运行过程中的信息安全风险。LIMS 本身服务于石化公司产品质量和生产安全，其系统本身更要有好的质量，包括完善的软件功能和投运后的较高的稳定性、可靠性。在网络环境下运行的信息系统，复杂性更高，在开发系统之前、开发过程中、系统运行时，都要注意信息系统的安全风险。

信息系统的安全风险，是指由于系统存在的脆弱性，人为或自然的威胁导致安全事件发生的可能性及其造成的影响。信息安全风险评估就是从风险管理角度，运用科学的分析方法和手段，系统地分析信息化业务和信息系统所面临的人为和自然的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和整改措施，以防范和化解风险，或者将残余风险控制在可接受的水平，从而最大限度地保障网络与信息安全。

信息安全风险评估是实现信息系统安全必要的步骤，通过信息安全风险评估，可以清楚业务信息系统包含的重要资产、面临的主要威胁、本身的弱点；哪些威胁出现的可能性较大，造成的影响也较大，提出的安全方案需要多少技术和费用的支持；分析出信息系统的风险是如何随时间变化的，将来应如何面对这些风险。

信息系统安全风险评估有三种形式，即自我评估、委托评估和检查评估。在 LIMS 系统中采用了自我评估方式。

在 LIMS 的实施与运行维护中，我首先确立 LIMS 的安全目标与策略，然后在风险分析中进行风险评估，在方案设计中对风险接受度进行评估，在安全计划实施中进行系统测评，在系统运行与维护中进行日常检查和定期评估，安全风险评估贯穿于信息系统安全管理的全过程，具有极为重要的作用。

在 LIMS 的安全风险评估工作方面，我采取了如下措施：

一、分析现有业务流程和新系统信息流的安全因素，做好安全风险分析。

为了全面了解新建 LIMS 系统的安全需求，我们仔细分析了现有业务流程各环节的安全因素，并通过对新系统信息流的来源、传输、处理和存储等环节的分析，识别 LIMS 系

统的安全风险，做好安全风险分析，为下一步的安全风险评估做好准备。

从 LIMS 数据的来源上看，基础数据来自于两种方式：手工录入；自动采集。通过各种化验分析仪器，产生了样品的分析数据，部分数据需要手工录入，部分数据通过采集器（如色谱采集器）进入系统，数据采集器的质量和化验员的操作水平会直接影响最后的分析结果，进而影响石化产品质量的判定，影响产品的出厂。部分化验分析仪器可以直接导出格式文本或 Excel 数据，这部分数据可以直接通过程序读取。数据收集过程的安全因素是必须逐个识别和分析的。

从 LIMS 数据的传输过程上看，网络设备（如 HUB、交换机、网线、光纤等）的质量是重要的安全因素，由于化验分析室中有毒、有害气体对网络设备腐蚀严重，一些重要的设备必须集中到工作环境相对较好的房间，在综合布线时必须考虑。每一个色谱数据采集器都要使用一个 IP 地址，部分化验分析仪器也要使用 IP 地址，IP 地址的管理不仅要考虑办公微机，也要考虑数采设备。网络安全是 LIMS 系统的重中之重。

从 LIMS 数据的处理和存储上看，许多分析计算要在 LIMS 客户端上完成，服务器上存放中间计算结果和最终结果（如审核过程和质量合格证），LIMS 查询机要应用在各生产车间和油品罐区操作室，操作员的素质和 LIMS 查询机的安全设置也是不能忽视的安全因素。

新系统投用后，业务流程会发生改变，比如会取消部分纸质台帐，审核方式也不再是人工审核，为了保证系统的正常运行，需要制定事故预案、应急措施，并要有系统运行管理部门。业务流程改变引发的管理方式改变，会造成许多不确定的安全因素。

二、建立安全风险评估标准，对安全风险评估分级、分类。

识别安全风险之后，就要进行风险评估。在风险评估过程中全面评估资产、威胁、脆弱性以及现有的安全措施，分析安全事件发生的可能性以及可能的损失，从而确定信息系统的风险，并判断风险的优先级，建议处理风险的措施。

风险评估是分级防护和突出重点的具体体现，有些风险可以接受，有些风险则要消除。每个风险的解决成本是不一样的，必须综合考虑。不存在绝对的安全，也不可能做到绝对安全。安全是风险与成本的综合平衡。盲目追求安全和完全回避风险是不现实的，也不是分级防护原则所要求的。

我们参照《信息安全风险评估指南》，结合 LIMS 项目的实际情况，建立安全风险评估标准，用定性和定量的方法为涉及到的安全风险进行评估，可以分级、分类，确定风险等

级和优先风险控制顺序，在评估结论中指出所有安全隐患，并给出解决方案建议。在对 LIMS 查询机的安全风险分析中，我认为操作员有可能通过 WEB 上的恶意访问和在 LIMS 查询机上的非法操作影响 LIMS 整个系统的运行，对几个解决方案进行了分析，认为在普通微机上进行一些安全设置，屏蔽掉一些多余的功能，比较可行，成本也低，而采用无盘工作站方式虽然安全效果更好，但成本太高，参照评估标准，选择最优的解决方案。

数据库服务器的安全风险级别较高，我们采用了双机热备软件，通过镜像引擎将数据由专用的直联线进行实时复制，当一台服务器发生硬件或软件故障时，自动启用另一台服务器，保证数据存储的安全和 LIMS 的长周期运行。

优先解决级别高的风险，是安全风险评估分级的目的。

三、在信息系统的各个阶段，反复对安全风险进行评估。

信息系统的安全是一个动态的复杂过程，它贯穿于信息系统的整个生命周期，对信息系统进行不断的安全风险评估是十分必要的。在 LIMS 系统规划设计阶段，通过风险评估明确系统建设的安全需求和安全目标；在验收阶段，通过风险评估验证信息系统安全措施能否实现安全目标；在信息系统运行维护阶段，定期进行风险评估，检验安全措施的有效性及对安全环境变化的适应性，以保障安全目标的实现。

LIMS 系统在 12 月底通过验收，正式投入运行，在两年多的运行期间，没有发生重大安全问题，LIMS 系统的建设、运行中的安全风险评估起了很大作用，明确的安全需求，合理的安全体系，严格的安全评估，灵活的安全措施，是系统安全运行的保障。

风险评估在信息安全保障工作中具有不可替代的地位和重要作用，我们在 LIMS 安全风险评估中采用的评估标准来源于多年信息系统实施和运行中积累的行业经验，并不是国家标准，还需要进一步完善，还存在着一些问题需要加以解决，如建立完善的工作机制、提高评估能力和技术水平等。信息安全风险评估是一项长期的工作，还有很多问题需要在实践中不断摸索，在理论中深入研究加以解决。