分类号_____ 密级 _____

UDC _____

学 位 论 文

首钢冷轧罩退信息系统集成项目风险管理研究

作 者 姓 名： 崔芳颖

指 导 教 师： 张吉善 副教授

东北大学工商管理学院

申请学位级别： 硕士 学 科 类 别 ： 专业硕士学位

学科专业名称： 项目管理

论文提交日期： 2012 年 6 月 19 日 论文答辩日期： 2012 年 6 月 17 日

学位授予日期： 答辩委员会主席： 杜晓君 教授

评 阅 人 ： 田扬 副教授 来振华 高级工程师

东 北 大 学

2012 年 6 月

A Thesis for the Degree of Master in Project Management

Research on Risk Management of Shougang Cold Rolled Baking Line Information System Integration Project

by Cui Fangying

Supervisor: Associate Professor Zhang Jishan

Northeastern University

Jun 2012

独创性声明

本人声明，所呈交的学位论文是在导师的指导下完成的。论文中取得的研究成果除加以标注和致谢的地方外，不包含其他人已经发表或撰写过的研究成果，也不包括本人为获得其他学位而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示谢意。

学位论文作者签名：崔芳菲

日　　期：2012年6月17日

学位论文版权使用授权书

本学位论文作者和指导教师完全了解东北大学有关保留、使用学位论文的规定：即学校有权保留并向国家有关部门或机构送交论文的复印件和磁盘，允许论文被查阅和借阅。本人同意东北大学可以将学位论文的全部或部分内容编入有关数据库进行检索、交流。

作者和导师同意网上交流的时间为作者获得学位后：

半年□　　一年□　　一年半□　　两年☑

学位论文作者签名：崔芳菲　　导师签名：

签字日期：2012年6月17日　　签字日期：2012.7.11

首钢冷轧罩退信息系统集成项目风险管理研究

摘 要

信息系统建设在钢铁企业中是一项错综复杂的综合性工程，是技术和管理等多方面工作的结合。目前首钢集团基本上完成了信息化系统建设，主要由4层结构组成，从基层机组自动化到整个生产过程控制，再到制造执行MES，最后到企业ERP的建设，已经把分散在各地的信息数据孤岛逐渐融合起来，实现了数据的高度集中，形成了一个全局的系统和架构。本文通过对目前国内外关于集成项目风险管理内容的深入研究，结合首钢顺义冷轧新建罩式退火项目的建设现状，运用项目管理知识对首钢冷轧罩退信息系统的构架和建设过程进行分析，对首钢顺义冷轧公司未来的发展具有重要而深远的现实意义。

本文在详细了解首钢冷轧罩退信息系统集成项目的基础上，通过对国内外集成项目风险管理的探寻和了解，对原冷轧信息系统的现状进行分析，明确首钢冷轧罩退信息系统集成项目风险管理的重要性和必要性；运用检查表、风险矩阵、风险计算等项目风险管理的基本方法对首钢冷轧罩退信息系统集成项目进行风险识别，确定出项目风险的具体范围并及时制定风险应对的措施。重点是从项目的风险分析和评估入手对首钢冷轧罩退信息系统进行研究，在项目的整体实施过程中将项目所涉及到的各个不同阶段的所有风险整合到一起集中进行项目的战略部署，分析和量化项目中的风险因素并对对项目的风险应对措施进行管理。得出在信息系统集成项目中以整体结果最优为目标进行风险分析、评估、防范风险发生的安全配置策略和防护原则。

论文研究得出的信息系统集成项目中的防范风险发生的安全配置和防护原则，对正在建设中的首钢冷轧公司具有极强的实际意义。使冷轧公司能够更好地借助信息化系统资源，深化管理，实现系统优化、措施到位，不断提升冷轧公司的市场竞争能力。

关键词：风险管理；集成项目；风险评估；风险控制

Research on Risk Management of Shougang Cold Rolled Baking Line Information System Integration Project

Abstract

Iron and steel enterprise information system is a complex project, it is both at technology based project is a managed project, Shougang Group is basically completed the four layer steel information system construction, from basic automation to the production process control, to the Manufacturing Execution MES,and finally to the construction of the enterprise ERP has information data islands scattered around the gradual integration together to achieve the data set to form a system of systems and architecture. In this paper, in-depth study of integrated project risk management, combined with the construction of the project of Shougang cold rolled hood retreat status, Shougang cold rolled cover back integrated information system architecture and construction process to analyze the use of project management knowledge, Shougang cold rolling the future development of profound significance.

In this paper, on the basis of detailed understanding of the Shougang cold rolledhood retreat integrated information system project to explore and understand the risk management of integration projects at home and abroad, the original cold-rolled the status of information systems for analysis, a clear Shougang cold rolled hood retreat integration information system importance and necessity of risk management; use of checklists, risk matrices, risk calculation of risk management on risk identification,Shougang cold rolled hood retreat integrated information system project to determine the scope of the project risks, develop risk coping strategies. Focus on integrated information system, Shougang cold rolled hood retreat from the risk assessment of the project to start research projects at different levels and different departments, all of the risks of the different stages of integration into the strategic planning of the project throughout the implementation of project activities and role of , to analyze and quantify the risks of the project, management of project risk response. Obtained in the integrated information system project is aimed at optimizing the overall results of risk analysis, assessment, prevention security risk allocation strategy and protection principles.

The paper studies the security configuration and protection principles of risk prevention,

Shougang cold rolled under construction with a strong practical significance. Cold-rolled better using the information system resources, deepen management, system optimization measures are in place and improve competitiveness in the market for cold-rolled Company.

Key words: Risk Management; Integration Project; Risk Assessment; Risk control

目 录

第1章 绪论

1.1 研究的背景

随着信息技术的高速发展和全球一体化进程的加剧。信息一体化已成为世界大发展的必然趋势，信息化时代的到来加剧了人类社会由工业时代向前发展的脚步。特别是21 世纪以来，中国信息化建设的步伐加快，各种信息系统已成为国家关键部位的基础建设部件。依赖网络的特点使信息系统的建设风险凸现出来，脆弱的信息系统对关键基础设施建设构成直接风险。同时，各个信息系统的建设已经由传统的PC 单独运行和封闭区域网络转向 Internet、无线网络、数据仓储等多种信息技术集成系统，这种信息技术集成系统的特点即复杂、开放、共享等，彻底改变了传统系统安全风险的本质，使信息系统项目建设和保证业务能够持续稳定运行面临着更大更高的风险。

国民经济中钢铁企业是其最重要的组成部分，随着信息一体化时代的到来，钢铁企业信息化的步伐也正在逐步加快。信息系统项目的实施为企业增强持续发展能力提供了抓手，也是提高企业竞争力和管理水平的重要途径，在不断发生变化的社会环境中，不仅应该注意到信息系统项目的优点，同时不应该忽略掉信息系统项目在很多方面所存在的风险，如管理方面、技术方面、建设的进度方面、维护力量是否充足等。而企业在信息系统项目建设的过程中要综合考虑到项目的很多特性，如管理过程的复杂性、信息系统工程项目的综合性和不确定性等等。伴随着项目管理理念研究的逐步深入，项目风险管理的意识也逐步由西方发达国家向发展中国家普及并向全球化合作方向发展。许多企业的风险意识明显增强，逐步在企业中增设风险管理机构，并专门配备风险管理经理、风险管理顾问，负责企业的风险识别、风险测定和风险处理等工作[1]。

1.2 选题的意义

近年来钢铁企业信息系统建设由萌芽期逐渐步入成熟期，信息系统的应用范围已经逐步从生产环节慢慢向服务性环节延伸。信息系统建设在钢铁企业中是一项错综复杂的综合性工程，是技术和管理等多方面工作的结合。所谓技术型项目必须以先进信息技术为手段，整体而全面的设计理念，合理而科学的技术构架等诸多对项目建设结果起决定性作用的因素组成。所谓管理型项目是指企业实施信息化将使管理手段发生根本性变化，导致企业的管理方法发生变革。企业信息化建设过程中一般会采用先进和成熟的商

业软件，因为这类软件是在众多企业的应用中获取了出了最先进的管理理念。首钢集团已经基本上完成了4层钢铁业信息化系统的建设，即从基础自动化到生产过程全流程控制，再到制造执行MES系统，最后到企业ERP系统的建设，已经逐步把分散在各个基地的信息数据逐渐融合，实现了数据集中，形成一个体系化的系统和架构。2007年投产的首钢冷轧薄板有限公司拥有国际先进的现代化设备，自动化水平高，产品众多，工艺复杂，因此需要全面的信息化集成系统予以配合。

通过对该项目实施风险的研究，来规避可能出现的问题，达到使冷轧的管理链条不断延伸，管理思路和过程不断得以细化的目的，将冷轧公司管理向的科学化和规范化推进。不断提高挖掘数据信息和资源的能力，充分利用信息系统进行数据分析、数据挖掘工作，加强业务分析能力，实现产品盈利能力分析、产品质量持续改进、合同交货周期分析等功能，不断提高为客户的服务水平。按照信息化建设“三流合一”的原则，运用信息化系统平台强化分工序成本核算，做到细、准、实。在复杂的冷轧生产工艺、物料和成本构成的动态控制与核算过程中，要借助信息化系统资源，深度开发和应用，算清成本账，持续降成本；实现成本可控、系统优化、措施到位，不断提升冷轧公司的市场竞争能力。

1.3 研究的内容

本文在详细了解首钢冷轧罩退信息系统集成项目的基础上，通过对国内外集成项目风险管理的探寻和了解，对原冷轧信息系统的现状进行分析，明确首钢冷轧罩退信息系统集成项目风险管理的重要性和必要性；运用检查表、风险矩阵、风险计算等项目风险管理的基本方法对首钢冷轧罩退信息系统集成项目进行风险识别，确定出项目风险的具体范围并及时制定风险应对的措施。重点是从项目的风险分析和评估入手对首钢冷轧罩退信息系统进行研究，在项目的整体实施过程中将项目所涉及到的各个不同阶段的所有风险整合到一起集中进行项目的战略部署，分析和量化项目中的风险因素并对对项目的风险应对措施进行管理。得出在信息系统集成项目中如何以整体结果最优为目标进行风险分析、评估、防范风险发生的安全配置策略和防护原则。具体的研究内容以下：

(1)首钢冷轧罩退信息系统集成项目风险的识别和分析阶段。在对项目背景和项目特点的简要分析基础上，运用检查表、风险矩阵、风险计算等项目风险管理的基本方法对首钢冷轧罩退信息系统集成项目进行风险识别，确定出项目风险的具体范围。

(2)首钢冷轧罩退信息系统集成项目风险的评估阶段。在对项目风险已经初步识别

的基础上，通过逐个对可能发生的风险进行评估，确定出项目风险发生的可能性以及影响程度，作为风险管理和控制措施制定的依据。

(3) 首钢冷轧罩退信息系统集成项目风险的应对阶段。通过对首钢冷轧罩退信息系统集成项目的风险进行分析后，综合运用风险管理的多种措施进行风险控制，制定出相应的风险应对的措施，尽可能的降低风险的发生。

1.4 研究的思路和方法

本文首先从冷轧罩退信息系统目前的现状入手，引出对冷轧罩退信息系统集成项目实施中的风险管理，然后运用先进的项目管理方法、工具进行了识别、评估及应对。项目涉及的范围较广，对项目管理理念、软硬件建设及施工等方面有一定要求，本项目需要在实施过程中总结经验，整合与协调存在的各方面利益的冲突保证新项目顺利实施，论文的研究思路见图 1.1。

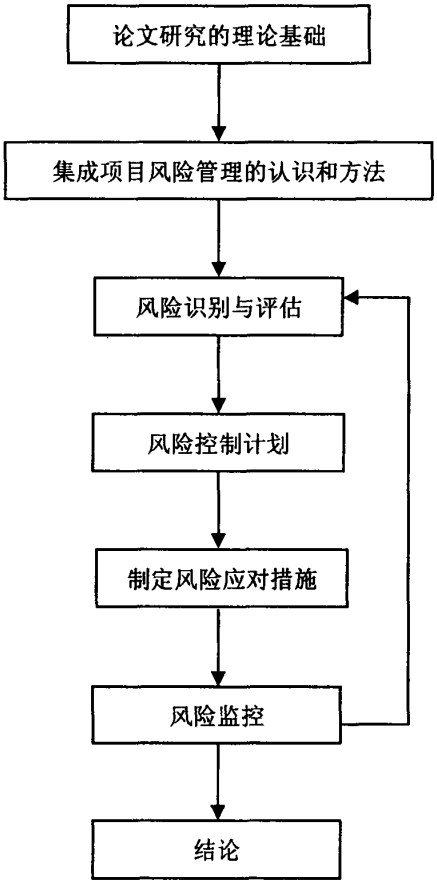

图 1.1 论文研究思路

Fig. 1.1 Research ideas of paper

主要采用了文献阅读、访谈、分类、观测、案例分析等成熟的研究方法对问题进行研究。

(1)文献阅读法。通过查阅、整理和搜集相关文献，并通过分析和鉴别找出所研究内容的科学依据方法。文献法是一种科学、有效的研究方法，它通过文献调研掌握有关的科研动态、前沿进展和已有的成果，然后对与现状有关的种种文献做出分析。

(2)访谈法。是通过与项目执行人员人面对面直接交谈来获取项目进展及问题的基本研究方法。因研究问题的性质、项目目的或访谈对象的不同而不同，访谈法运用面广，能够简单而快速地收集多方面的工作分析资料。

(3)分类法。主要是指以事物的不同属性作为分类的标准，如性质、特点、用途等，按照相互间的关系组成系统化的结构，用统一的标准将事物进行分类，区分出不同事物的方法。

(4)案例分析法。以首钢冷轧罩退信息系统集成项目为例，对项目风险进行识别、分析和评估，并有针对性地制定了风险应对措施，从项目的施工、工程质量和项目进度等方面进行有效的管控。

1.5 论文的结构

本文共分六个部分：

第1章绪论，概述了研究的背景、意义，介绍了研究的对象、内容与方法，并对论文研究内容和框架进行综述；

第2章相关研究理论综述，对项目管理、风险管理、集成项目风险管理等相关理论进行概述；

第3章首钢冷轧罩退信息系统集成项目风险管理概述，详细介绍了项目的背景、总体计划和特征，并针对存在的风险进行概述并提出相应的管理要求；

第4章首钢冷轧罩退信息系统集成项目风险识别与评估，对项目的风险因素进行识别，分析和评估风险点并将风险因素进行量化分级；

第5章首钢冷轧罩退信息系统集成项目的风险控制与应对，通过风险的控制目标和计划减少风险发生，当风险点爆发时用正确的应对措施进行应对以保证项目的顺利完成；

第6章结束语，简括了本文的主要研究结论和进一步展望。

第 2 章 项目风险管理的文献综述及基本理论方法

2.1 集成项目风险管理文献综述

2.1.1 国外研究现状

项目管理实践活动最早开始于 20 世纪 40 年代，美国将项目管理理念应用于研制原子弹的曼哈顿计划中。到了上个世纪 60 年代，项目风险管理的理论研究开始在世界各地的开展，美国项目管理协会(PMI)开发的项目管理知识体系指南指出，项目风险管理是指对项目风险从识别到分析乃至采取应对措施等一系列过程[2]。项目的风险管理是将项目实施中各项风险作业相互交叉重叠进行的一个动态工作过程。项目风险识别是项目风险管理的重要环节。若不能准确地识别项目面临的所有潜在风险，就会失去处理这些风险的最佳时机。

Shen8 通过的一项关于工期延迟问题的问卷调查结果，分析得出 8 个对工期影响重大的主要因素的权重，指出不充分和错误设计信息是导致工程延期的最主要因素，其次是地质和天气状况的变化，同时还给出了防止工程工期延误的 7 个最有效的方法。

2.1.2 国内研究现状

自上世纪 80 年代后，我国在项目建设上、工程实践中为项目管理研究迈出了第一步。1984 年鲁布革水庄站[3]就是利用了世界银行的贷款，在国内第一次采用了国际招标方式，推行了项目管理理念，起到了缩短工期、降低造价、取得经济效益的作用。同时，项目管理理念逐步向各行各业扩展，由国防航空领域逐步普及到金融、建筑，随着信息技术的发展，计算机、网络等行业也在逐步引入。进入 21 世纪以来，信息产业在政府的高度重视下得到很快发展，取得了一定的成就。信息产业的风险问题研究开始于风险决策，1987 年清华大学郭仲伟教授《风险分析与决策》的出版标志着风险管理研究的开始[4]。但是在计算机技术方面的应用看，很多软件设计公司开发的的风险管理有关的软件，虽然采用了计划和协调技术，但是没有针对具体的项目进行整体风险管理，而中国科学院研制的项目风险分析系统 PriskA[5] (Project Risk Analysis)也只能针对项目的一部分就行风险分析，而不能全面、深入的研究，毕竟项目风险管理所涉及的研究范围很

广，而在实际的项目实施过程中，存在很多不确定的因素，客观上让项目的风险管理遇到了阻力。因此在应用方面，具有系统性、完整性和专业性的集成项目风险管理研究就显得越来越重要。

目前项目风险管理的研究热点是集成项目风险管理、全生命周期风险管理和持续风险管理。项目风险管理研究主要是采取定性分析和定量评估相结合方法，建立起项目风险管理的框架，并针对不同层次的项目特点进行管理。集成项目风险管理，兴起于金融行业的项目管理当中，主要理念是对金融机构内所涉及的多种分类风险汇总管理，并把存在风险的各种资产组合、和产生风险的单位都统一进行考虑，根据风险管理的标准和工具对风险进行评估，然后根据有无相关性对风险进行统一的控制和管理，动态的、集中的考虑不同的风险。

谷秀娟[6]从金融市场管理的角度，总结出了全生命周期风险管理的优势是有助于对冲对风险起到降低的作用，来增加企业的盈利和降低成本，不是逐项的查找，是从整体综合考虑的结果。唐玲玲[7]结合工程建设的是实际情况，提出了建设工程项目中集成风险管理的模型，并将模型应用于提供项目建设咨询中，提出项目风险来源的分类。杨乃定在提出了基于项目集成风险管理的六要素，并在这六要素的基础上建立起的一种新型的企业集成风险管理模式，将战略、组织方法、信息和文化进行了集成。尹贻林[8]等在研究全周期集成化建设项目管理的基础上，提出了系统组织模型，克服了以前在项目实施过程中需要项目经理去协调各方关系的这个弊端，让项目实施过程中参与项目的各个组织有了一个集中的交流平台，提高了工作效率，让集成项目风险管理研究成为了可能。

2.1.3 集成项目风险管理的特点

知识、技术、经济等方面发展的全球化是世界一体化的一个重要特点，社会进步、竞争加剧、信息技术的快速蓬勃发展，促使项目的风险管理向全球一体化发展。日益增多的国际合作，频繁的项目共建和项目管理的信息共享等等，为项目管理研究走向全球一体化提供了渠道，加快了项目风险管理研究向高水平发展的步伐。风险管理研究位列项目管理的九大知识体系其中，一直以来都是学术界的热点研究。而今将本学科的专业知识理论、方法技巧如何和项目风险管理的相关内容、知识相融合，应用到具体行业当中去成为了项目风险管理研究的发展趋势。目前项目风险管理研究的内容主要集中在项目的费用和成本控制、工程进度、实施效果和质量目标的集成上。特别是针对在项目环境不确定的情况下工程项目相关问题的优化中，如时间、费用和质量等，在定义出来项

目目标风险度的基础上，利用模糊数学等理论，建立模型，利用遗传算法来进行优化和求解。

项目管理的特点，即复杂性、综合系统性和建设过程中的不确定性都迫切要求在工程项目建设过程中实行项目风险管理。项目风险管理研究即有理论研究的意义，又对现实工作有指导作用。静态而孤立，不从全局出发，只以项目的局部目标作为管理对象的工程项目风险管理方式已经不能适应现在社会的需要，因为这种研究明显忽视了集成风险管理体系的意义。集成项目风险管理需要将项目中的所有风险活动通过一个合理的模式有机的整合在一起，这种模式应该是建立在项目目标明确、组织方法和过程控制有效的基础之上。在此基础上用系统集成的方式进行思考，引入前后照应、左右协作的管理方式，提出项目的风险管理集成概念，以企业工程项目风险管理更有效，最终工程项目风险管理的整体最优为目的，用集成的概念来管理项目的运作过程和实施内容，以确保项目的顺利实施，达到项目完美收官。

2.2 项目风险管理定义及分类

项目风险管理是指对项目风险从识别到分析乃至采取应对措施等一系列过程，它包括将积极因素所产生的项目风险管理流程中的影响最大化和使消极因素产生的影响最小化两方面内容[9]。项目风险管理的过程强调的是对项目目标的一种主动控制，提前预防项目实施的过程中所能遭遇的风险及干扰的因素，以避免或者减少风险损失。具体项目的实施过程中，成功的风险管理将直接关系到项目管理的成功及项目目标的实现。风险管理的过程就是合理运用风险管理技术和方法来系统识别项目相关风险，有效控制和处理风险损失及后果的过程，以改善项目的执行效果。

传统的项目管理策略是孤立的分析，以概率评估为主要标准，而目前的项目风险管理则是以集成的思路进行思考，重视风险事件的发生过程及其后果中的偶然性、不确定性和可变相对性。合理运用集成项目风险管理的特点，在风险识别过程中充分合理利用风险的属性，使识别结果更加客观准确和全面。论文中利用文献法查找综合后结合研究内容划分风险类型为：

(1)依据风险因素和项目之间的关系可以分为内部风险、外部风险。

(2)依据风险因素对项目的影响范围可以分为全局风险、局部风险。全局风险将对项目的整个过程发生影响；局部风险只对项目中的的某一部分发生影响，涉及的范围较小。

(3)依据风险来源可以分为自然风险、人为风险。自然风险是不受控制的，一般是外界影响，如地震、海啸等。人为风险是包括政治、经济、技术、社会、管理等方面，可以是全局风险也可以是局部的。

(4)依据风险因素的不确定性可以分为可控制、不可控制风险；可预测、不可预测风险。可控制的风险是指与项目的实施过程直接有关的风险，如项目进度风险、安全风险、技术风险等。

(5)依据风险因素作用持续的时间可以分为暂时风险、长期风险。长期风险将影响整个项目周期，甚至项目结束后，且项目过程中发生频率较高。

2.3 项目风险管理的过程

项目风险管理主要经历四个过程，见表2.1：

(1)识别阶段：运用识别风险的专用方法和技术对项目建设过程中的的内部和外部环境来进行综合分析，对项目整个过程中可能面临的风险进行认识的过程。

(2)评估阶段：运用定性分析和定量分析技术相结合，分析风险识别结果的方式，评价风险因素发生的可能性及发生的风险对项目可能造成的影响。定性风险分析是对已经识别的风险发生的可能性和对项目的影响程度进行全面评价，并将风险对项目目标值的潜在影响程度进行排序的过程[10]。定量分析是建立在定性分析的结果之上的，主要是把项目中具体的风险因素发生概率和影响程度进行量化，以便可以对项目总体风险给予正确评价。

(3)应对计划编制阶段：利用项目风险分析识别和评估的结果，根据项目的具体管理要求和设计思路，制定出防范风险发生的各种措施，并根据措施来制定和选择对项目风险管理最有效的方案并付诸实施的过程。

(4)应对监控阶段：将制定出的风险应对措施应用到项目管理中实施后，对实施效果是否有效进行监控，并根据监控的结果及时调整风险管理的计划及具体项目要求，结合实际运作，监控阶段既是项目风险管理过程的结束，也将是进一步项目管理的全新开始。

表 2.1 项目风险管理框架

Table 2.1 Project risk management framework

过程	依据	工具和方法	输出
风险识别	环境因素和组织因素	德尔菲技术	已识别风险清单
	组织过程资产	头脑风暴法	潜在应对措施清单
	项目范围说明书	SWOT 分析法	风险基本原因
	风险管理计划	检查表	对风险类别的更新
	项目管理计划	图解技术(如因果图、系统或过程流程图等)	项目管理计划(更新)
		文档评审	
		假设分析	
定性风险分析	组织过程资产	风险概率与影响评估	风险清单(更新)
	项目范围说明书	概率和影响矩阵	
	风险管理计划	风险分类	
	风险清单	风险紧急度(紧迫性)评估	
	工作绩效信息	风险数据质量评估	
定量风险分析	组织过程资产	期望货币值(EMV)或决策树分析	风险清单(更新)
	项目范围说明书	计算分析因子	
	风险管理计划	计划评审技术(PERT)	
	风险清单	蒙特卡罗分析(或建模与仿真)	
	项目管理计划	访谈	
		概率分布	
		专家判断	
风险应对计划编制	风险管理计划	消极风险的应对策略——回避、转移与减轻	风险清单(更新)
	风险清单	积极风险的应对策略——开拓、分享和增强	相关的合同和协议
		风险接受的策略	
		应急响应的策略	
风险监控	项目的管理计划	风险再评估	风险清单(更新)
	风险的管理计划	风险审计和周期性风险评审	新的变更申请
	风险清单	偏差和趋势分析	建议的纠正措施
	工作绩效信息	技术绩效衡量	组织过程资产(更新)
	已批准的变更请求	储备金分析(或预留管理)	推荐的预防措施
		状态审查会	
		风险预警系统	

2.4 项目风险管理的方法

风险管理的不同阶段，应该运用不同的工具和方法，主要介绍论文中所采用的项目风险管理的工具和方法：

(1)风险识别阶段，主要用到的是头脑风暴法和检查表。

①头脑风暴法是指当讨论具体风险因素时，项目管理成员逐个说出自己的观点，并

有成员协同记录所叙述内容，不断重复这个过程，管理成员不断表述观点，规定时限或者一直到没有新观点产生。这种方法可以调动和利用团队成员的创造性思维来设计具体方案，广开思路，集思广益。

②检查表是基于相似项目信息编制的风险识别因素表。检查表通常按照风险的来源进行排列。利用检查表进行风险识别的主要优点是快而简单，缺点是受到项目可比性的制约，见表 2.2。

表 2.2 检查表
Table 2.2 Checklist

分类	风险名称	所含风险因素	可能性	严重程度

(2) 风险评估阶段，主要用到的方法有主观概率评估法、模糊数学法、影响矩阵。

①主观概率评估法。主观概率评估是指用主观概率对风险进行估计，表现为风险发生前对时间后果迅速判断的个人观点，用数值来描述时间的发生可能性和发生后所带来的后果，需要的信息量少。需要经验丰富的专业人士进行评估，但与实际风险可能存在偏差，最好是多人参与，多次评估。

②模糊数学法。风险的不确定性决定了在风险评估过程中，很多外部的影响因素的性质和内容无法用数字定量的表述，也无法用单一的准则进行判断。因此用概念化的数学语言去分析和解决，将模糊的问题量化，可以增加评估的准确性。但这种模糊的数学关系的如何量化及数学化，还是需要有经验的专业人士给出。

③风险矩阵是将风险发生的概率和风险对项目影响的可能性分别作为矩阵的参数，对风险的重要程度进行判断，优点是直观简洁。

2.5 集成项目风险管理的发展趋势

近年来，学者从微观视角，提出了全面风险管理概念，对建设项目风险的识别和预防有着积极的意义。进入 21 世纪后，风险管理的理论和实践研究得到了极大的发展，特别是计算机、网络技术的飞速发展，为风险管理思想应用实际的技术发展提供了极大的支持，促进了风险管理理论的深入、应用的普及。全方位、全生命周期的、动态的风险管理将成为未来风险管理的发展趋势[4]。

同时，工程项目的复杂性决定风险分析不能采用单一方法来进行，根据工程项目风险管理的特点，应该采用多种方法结合来进行项目风险分析。目前，对风险管理的研究以“集成”为主流，传统的“分裂式”发展的思想逐步被“整合集成式”发展的理念取代[11]。在这种发展趋势下，近几年，在风险管理的实践中，项目风险管理的集成化也逐渐成为业界讨论的热点。但从综合文献了解到的研究现状看，集成项目风险管理的研究尚存以下不足，将成为未来该领域研究的重点：

(1)集成项目风险管理的理论体系目前还不完善。尽管有学者对集成项目风险管理的模式进行了研究，提出了一些集成风险管理的理论框架，但对于理论框架内部的构成以及他们之间的相互关系还缺乏深入细致的讨论，从而制约了集成风险管理理论的更好的应用。

(2)集成项目风险管理的理论研究开展的还不够深入，仅仅停留在概念性的讨论层面。虽然项目风险管理的集成化已经成为必然趋势，但是对于项目风险管理如何“集成”这样的具体问题深入研究的还较少，而且不够深入，缺少对工程项目集成风险管理方法的研究。

(3)集成项目风险管理各方面的研究发展不均衡。项目目标集成方面和单一风险管理方法与专家知识库系统的集成方面研究开展较多，但对于项目各方的组织集成以及项目风险管理信息系统方面则开展较少，这与项目集成风险管理理论体系不完善是有关系的。

第3章 首钢冷轧罩退信息系统集成项目风险管理概况

3.1 首钢冷轧罩退信息系统集成项目背景

08 年全球性金融危机后我国钢铁行业也出现萎缩，钢铁市场出现严重的供大于求现象，首钢集团由于兑现奥运承诺，限制和约束产能，搬迁调整等面临着巨大的内外部压力，现实要求首钢集团必须加快寻找出路的步伐，通过强化管理来挖潜增效。目前国内主要的钢铁企业都在加快信息化建设的脚步，希望通过信息化手段来降低成本、提高生产效率和增强企业的核心竞争能力。面对竞争，首钢集团为了在激励的市场竞争中立于不败之地，也迅速利用信息化手段来增强自身的竞争力。2003 年首钢集团开始进行信息化建设，引进先进的管理思路和模式，应用先进的信息技术手段，在对全首钢集团进行信息业务再造的基础上对钢铁主流程实行 ERP 系统全流程管理，建立起了融合了企业管理与信息管理相结合的现代化的管理模式，实现了以财务管理为核心的 ERP 系统。目标是在业务操作层面实现企业物流、资金流、信息流、工作流的全面集成，实现企业业务流程的信息管理；全面应用计算机网络及各方面的先进 IT 技术，以达到管理手段的现代化；在整合资源配置层面，促进集团资源配置的集成与优化，促进全面提升企业的经济效益。首钢冷轧罩退信息系统集成项目就是在首钢现有信息系统的基础上增加部署实施的。

首钢集团是超大型的国有企业，随着首钢生产建设、搬迁调整、改革创新的不断发展，企业对信息化的要求和依赖性也越来越高，伴随着企业的进步首钢信息化建设事业得到了长足的发展。如今在首钢企业环境中运行着与企业生产、经营、管理密切相关的信息系统，ERP 系统、MES 系统、人力资源管理 HR 系统、办公自动化 OA 系统、企业网站、企业邮箱、客户营销服务平台等，这些新型的管理系统的应用给企业带来更高生产效率的同时也对所处的网络环境和信息系统安全提出了新的要求。目前首钢北京地区已经停产，搬迁调整工作基本完成，今后在总部经济、一业多地的发展格局下，企业未来的生产经营、业务开展对信息系统的依赖性将更加显现，维系首钢一业多地企业信息网络系统的安全则显得更为重要。企业信息系统由于安全问题造成破坏而将严重损害企业法人的生产、经营、管理等利益，对社会也将产生影响。根据首钢的企业规模、社会影响等因素，根据首钢企业网络的规模和复杂性，根据首钢企业信息化应用系统数量和重要性，为确保首钢企业信息环境的安全和业务系统的持续稳定运行，有必要对首钢

目前企业信息网络系统环境的安全状况进行充分地梳理，通过进一步开展信息系统的安全风险评估工作对存在的问题和差距有一个清醒的认识。希望在对首钢信息安全风险评估结论的基础上得到改进措施和解决方案，使自己找到差距，发现漏洞，制定措施，及时改进，达到要求，以便使企业的信息系统和网络环境的安全状况得到明显的改善和提高。

3.2 首钢冷轧罩退信息系统集成项目的总体计划

2008年5月具有170万吨冷轧板生产能力的首钢顺义冷轧公司酸轧、连退和2条镀锌线全面投产，具备和集成了国内外最先进的生产工艺和高新技术，整体技术和装备水平居当今世界前列。按照首钢总公司整体发展规划，为了提高首钢冷轧公司产品市场竞争力，结合公司目前产能不匹配情况，在现有生产设备的基础上，增建罩式退火机组。

首钢顺义冷轧建设罩式退火炉生产线的必要性。对于普通冷轧板生产，轧后冷轧带钢的处理有两种工艺，具体流程包括脱脂电解机组、罩式退火炉炉台机组、单机架平整机组、重卷及包装等独立生产机组，和以钢卷为单位的分批处理生产流程。在罩式退火的工艺中，强循环的全氢罩式退火炉代表着现代罩式炉技术的最高水平，较传统的N2+H2 罩式炉在退火效率、退火质量上有质的突破，缩短了罩式退火与连续退火的差距，因此罩式退火工艺流程在冷轧带钢退火中具有独立地位。因此在现代新建的罩式退火项目中都会选用全氢罩式退火炉。罩式退火在生产灵活性，产品规格限制小，利用常规钢种生产优质、低成本深冲及超深冲产品等方面有其独特性，是大型钢铁企业中对连续退火项目的的必要补充。

罩式炉生产可使用普碳钢、铝镇静钢、中碳钢、高强度低合金钢、微碳烘烤硬化钢等多种钢种生产多种普通冷轧产品，特别是利用铝镇静钢生产深冲、超深冲产品用作汽车板、家电板，不仅产品的抗时效性优于连退产品，而且生产成本可以大大降低，相同水平下比连退使用IF钢低能够低300元/t。罩式退火炉方案主要包括：市场情况初步分析、项目的产品定位和产品大纲、生产工艺和设备组成、公辅设施配套、总图运输和物流、平面布置和项目投资。针对罩式炉不同产能与冷轧配套生产能力进行了经济技术比较分析，最终确定为60万吨方案，产品定位为汽车板、家电板和特性产品，生产这三样板的比例分别为汽车板60%、家电板25%和特性产品15%。首钢顺义冷轧罩式退火项目的总投资大约为6亿元，设计指导思想和原则是以市场为导向，巩固公司现有产品市场基础上，积极开拓市场上急需的家电板和汽车板等普通冷轧板带产品。采用“先进、

可靠、适用”的工艺技术和装备，达到现代化的装备控制水平，具备在国内外两种市场上竞争的能力。在部分需要引进技术和设备中，贯彻引进国内尚没有掌握或技术达不到性能要求的技术和设备。项目将坚持“高起点、投资省、质量好、工期短、见效快、环保优”的建设原则，在满足产品质量的前提下，以国产优设计为主导，降低建设成本，节约建设投资。

3.3 首钢冷轧罩退信息系统集成项目的特征

项目的总体目标是将新建罩退线纳入现有的ERP平台进行管理,实现企业资源的统一集成高效配置；在现运行的顺义冷轧的 MES 软件产品的平台上进行扩展，实现罩退产线的生产计划排产、产线排序、生产工艺执行、仓储运输管理、接口管理、报表管理等。信息化网络覆盖新建的罩退产线，搭建经营生产管理完整的信息化基础平台。

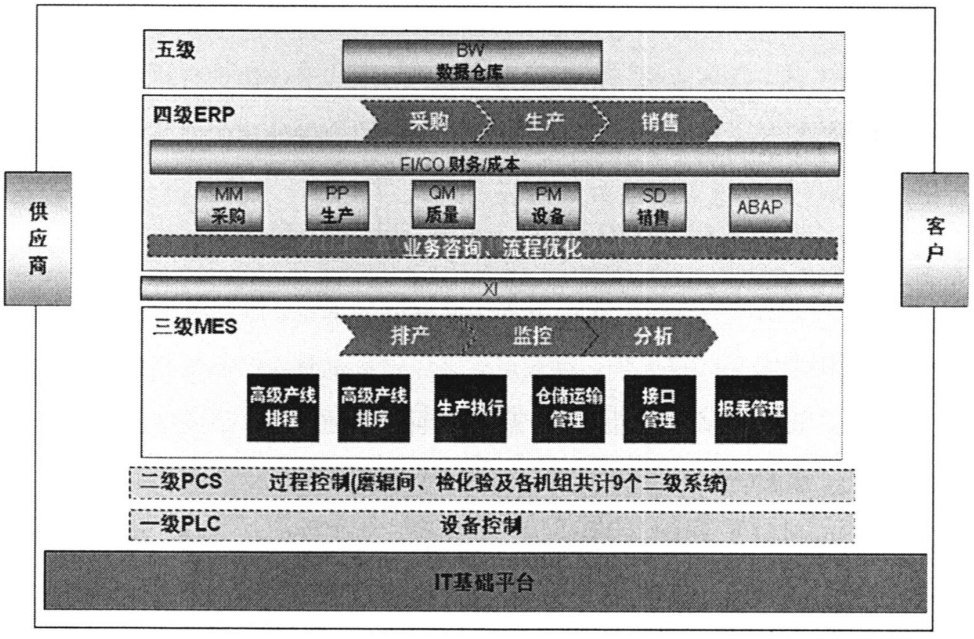

图 3.1 项目的信息化布局

Fig. 3.1 The layout of the information technology

ERP 主要目标是将顺义新建的罩退产线及拓展业务(平板产品)相关的业务按照已实现的流程纳入现运行的 ERP 统一系统平台，实现物资供应、生产和销售、质量、财务成本、设备备件业务的信息共享和数据集成。实现 ERP 系统与现有各应用系统及 MES 系统的全面信息贯通；实现与总公司相关的系统业务集成。实施模块包括基于 SAP 平台的财务管理(FI)、成本管理(CO)、销售管理(SD)、生产管理(PP)、质量管理(QM)、采购供应管理(MM)、设备检修管理(PM)、备品备件管理(MM)、报表开发(ABAP)、

数据仓库(BW)、接口中间件管理(XI)。

MES 主要目标是冷轧罩退信息化，是在冷轧现在运行中的 ERP、MES 系统中，保持业务模式和流程不变的基础上实施之；考虑到顺义冷轧未来实施一体化质量设计的情况(将对现有 MES 产生很大的改动)；因此，针对罩退 MES 的设计和实施，采取简化的原则。技术方案利用现有 PES 扩充进来脱脂、罩退、平整、重卷机组，并在 PES 平台开发简化的计划排序功能，满足罩退生产的业务需求。实现冷轧罩退产线生产一体化集成，对脱脂、罩退、平整、重卷等各个工序的生产过程进行有效计划和控制，并以此进行实时动态调度，和销售紧密联系。实施内容包括顺义 MES 系统扩充：订单技术展开、脱脂机组排程、罩退机组排程、平整机组排程、重卷机组排程、生产执行、仓储管理系统、MES 系统与各产线机组的接口。

IT 主要目标是随着冷轧罩退工程项目建设的展开，为了满足以后三、四级系统在冷轧厂的应用，需要把基础信息化网络覆盖到各个罩退办公区、库管室、操作室和电气室。同时对冷轧现有服务器系统进行扩容，以满足三四级应用需求。实施内容包括顺义冷轧罩退网络汇聚层机房建设(图 3.2)、接入层、无线 AP 的设计及系统集成、光缆敷设、网络综合布线、终端安装、服务器、存储扩容等。

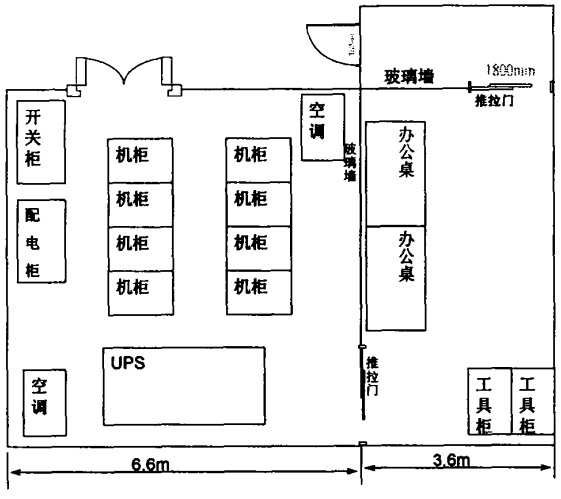

图 3.2 首钢顺义冷轧罩退新建网络汇聚层机房布局

Fig.3.2 New engine room layout of the network aggregation layer

3.4 首钢冷轧罩退信息系统集成项目的风险管理目标

在初步分析了首钢冷轧罩退信息系统集成项目的风险后，根据项目的实际情况提出

对项目的具体管理要求：

(1) 网络安全

网络核心交换设备部署性能是否良好，重要设备和链路都是否有冗余设计，是否具有与实际网络相一致的网络拓扑结构图，网络管理员定期对网络拓扑(见图 3.3)进行修订，便于工作人员掌握网络结构的整体情况，但可能不是非常及时，因为各系统管理员职责不同，沟通上存在延迟；网络内按照不同楼层、工厂内现场区域划分成不同网段和 VLAN；目前终端的控制强制使用北信源，计费，防病毒网管，对于重要应用系统可限制访问，访问控制范围由冷轧信息部制定；部署防病毒网关，能对 HTTP、FTP、SMTP、POP3、imap 等协议进行控制；所有使用者的客户端使用北信源策略进行 MAC-IP 硬件地址的绑定，防止地址欺骗。

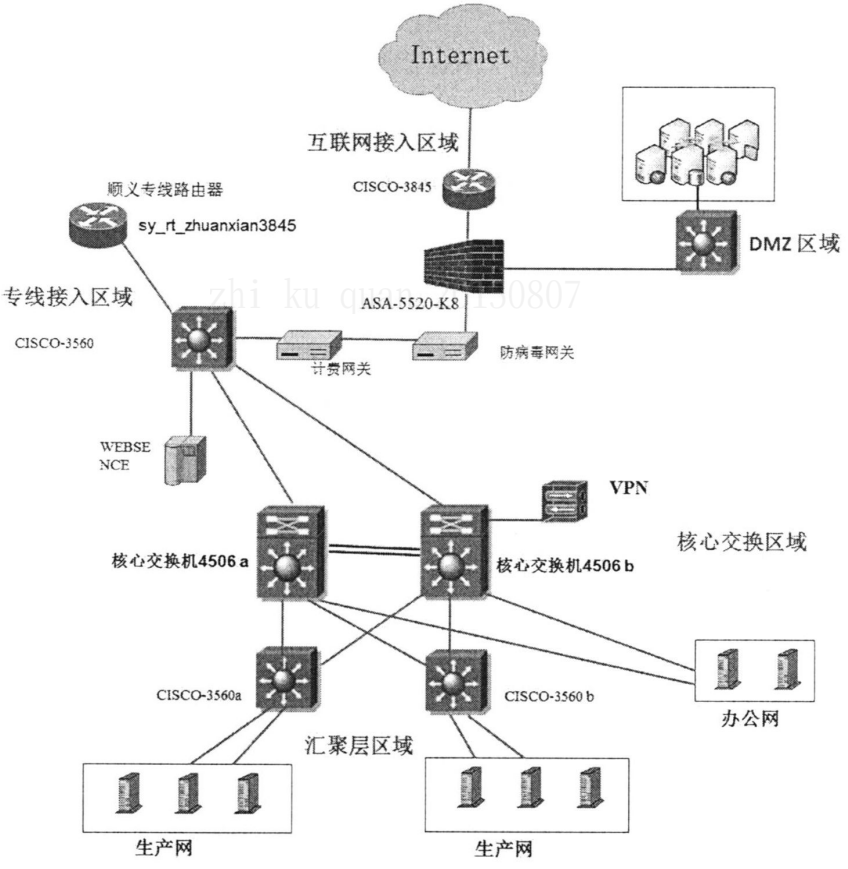

图 3.3 首钢顺义冷轧网络拓扑图

Fig. 3.3 Shougang cold rolled network topology

(2) 应用系统及服务

①MES 系统

使用用户名密码对登录用户进行身份标识、鉴别和登录控制；提供用户身份标识唯

一性和鉴别信息复杂度检查功能，用户身份鉴别标识与员工姓名对应；系统根据用户的用户身份标识标志及登录失败处理功能，配置相关安全策略参数；设置访问控制功能，依据不同用户的岗位职责划分，表现在登陆界面不同；系统管理员严格根据用户访问的业务需求，赋予相应的访问权限，相关访问主体的权限目前由工作岗位来决定，一般为最小化权限配置；系统使用实名账户，有策略的配置能力，严格控制各组织机构相关人员的操作权限；系统提供覆盖到每个用户操作记录的安全审计功能，并对应用系统的除查看查询操作之外的所有操作项进行记录，审计记录一直保存，需要时手工查看；系统对输入的数据有效性进行检查，对输入数据格式有要求，对错误输入有提示；设置系统的最大连接数为200，消除长期挂在系统中占用资源的情况发生，设置自动结束回话机制。

②办公系统

网页的后台提供登录控制模块，使用不同的用户名密码对登录用户进行身份标识和鉴别；根据不同岗位职责，划分不同的访问权限，提供了必要的访问控制功能，目前分为领导权限和普通员工权限，根据不同的发文类型和各节点的权限属性来控制操作；OA系统管理员为默认账户，由管理员进行访问策略的修改，对于各种用户帐户访问限制；系统为每个用户提供安全检测功能，并对日志记录每个应用系统的安全事件；审计记录包括日期、时间、发起者帐户信息、操作环节、通过工作流程可追溯到户用的操作。

(3)信息安全管理

信息部负责冷轧厂信息系统，按照系统划分不同的系统管理员，明确职责，但是一个人管理一个系统的所有事物。顺义基地信息部和首自信的工作分工主要是信息部负责运行管理，而首自信人员主要负责具体的运维操作。首自信维护人员对各种系统进行日常巡检，通常机房一天巡检4次，首自信人员每月将系统运维报告发送给信息化管理办公室，顺义信息办每周查看巡检记录，有时也会对去机房查看机器运行情况。顺义基地信息办和首自信相关人员开月例会。信息办系统运行管理员会不定期对首自信人员的工作进行监督检查，主要是和相关负责人讨论系统安全运行情况，看当月有哪些故障和问题，安排下月工作部署；对于系统变更或者升级审批，除四级系统以外的变更有总公司来审批，其他的事务均有顺义信息办负责审批。顺义信息办人员主要参加北京市政府、总公司、顺义区政府等组织的安全会议，很少参加同行业信息安全会议。

(4)人员管理

顺义冷轧员工主要是由冷轧公司自己录取，首自信维护人员由首自信录取，但是在

维护协议上会规定主要人员的名字和人数，所以工作人员和维护人员都会要求与公司签订保密的协议和岗位安全协议。顺义地区员工在办理离职手续时要先到信息办注销用户和权限，在离职手续单上需要有信息办签字盖章后才能办完离职手续；目前顺义冷轧没有针对员工进行过信息安全知识和技能培训，但是进行安全制度的培训。信息化管理岗的培训通常都是有总公司来进行，对于安全产品(例如北信源、趋势、防垃圾网关、内容过滤)的培训有总公司组织，厂家工程师来介绍。对于员工的安全考核，通常在重大节日前进行普查或者一个季度普查一次，也只是偏向于生产安全操作、上网行为控制以及使用 U 盘等方面，不是对于信息安全意识和技能方面；对于外来人员的管理，目前没有明确的管理制度，外来人员进入机房时必须先进过信息办的批准由信息办的人员或者委托首自信陪同，但是没有机房外来人员登记。

(5)系统建设

顺义冷轧的信息化建设由信息化管理办公室全面负责，通常建设方案中的安全策略由信息化管理办公室提出，经总公司批复后，由首自信负责编写建设方案，方案完成后会有专家对其进行 2 轮的评审；对于安全产品的选型一般来讲，如果在前期工程中总公司有统一品牌，那么在后期工程中会继续沿用，如果是新设备的选型，则有由首自信出具技术方案，顺义信息办把详细方案报给总公司，有总公司的相关领导来决定方案是否能通过。产品的采购主要通过招标的形式，由顺义冷轧信息办、首钢信息部以及首自信共同决定；目前顺义冷轧 ERP 系统、MES 系统的软件基本上都是直接购买国外产品，首自信实施安装。通常没有保存源代码，也没有审查软件中可能存在的后门，软件的运行状况由首自信负责，信息部偶尔会抽查；信息化建设过程中，由信息化管理办公室负责对工程的实施进行监督管理，没有第三方监理。信息化建设完毕后，信息办组织相关业务部门对此系统进行安全性测试并出具测试报告，但主要是内部测试，没有第三方单位对系统(包括硬件、软件)进行安全性测试。项目验收后，建设单位是否会提交系统交付清单、建设文档、运维指南等相关文件；由于信息化管理办公室人员不足，因此在信息系统的架构、规划和建设过程及后期运行维护过程中无法对系统的建设进行有效监督检查，目前没有书面规定出系统验收、系统交付的控制方法及系统将来维护的方法和人员行为准则等。

(6)系统运维

有专人负责机房安全，但是没有专职机房管理员，通常机房巡检每 2 小时巡检一次，主要是检查服务器、UPS、核心交换机以及空调温湿度等运行状况，如果服务器出现故

障，首先会通知信息办，同时首自信维护人员会检查设备状态，初步判断故障原因，如果需要更换设备，则有信息化管理办公室通知设备维保人员；如果是应用系统或软件故障，首自信IT运维人员会初步推断故障原因并进行处理，如果处理不了的问题则上报信息办和北京二线支持人员；服务器用户名、密码一般都有首自信维护人员自己定，三级系统个人用户由各单位上报账号和权限，信息办批准制定后，由首自信开通；IP VLAN有首自信建设是规划，信息办审批，根据总公司统一设计。信息化管理办公室负责控制终端的信息安全。各个基地和总公司的策略由总公司信息部来规定；目前没有成文的设备安全管理制度，但是对设备领用规定的比较严格。有资产清单，但是管理界线比较模糊，有相关规定对资产进行进行标签登记，资产分类较明确，设备标签齐全，但是没有成文的《资产管理制度》。无相关介质安全管理制度，有专门的屋子进行保存，磁带放在顺义档案室。在《北京首钢冷轧薄板有限公司信息系统安全保密管理办法(试行)》规定了U盘的使用规范，规定工作站的U口封掉，但是服务器的U口没做处理，需要倒出报表的时候会用U盘直接插到服务器中倒出数据，没有申报流程。一般维护人员用的都是自己的U盘，很可能会带出公司。虽然在顺义冷轧生产网中禁用了U口，但是在办公网中没有禁用，通常在外网电脑中可以进入到生产网络中进行业务处理。暂时没有建立安全管理中心，只是使用北信源注册的方式对设备状态、补丁升级对安全内容进行管理，首自信维护人员对网络进行管理，主要负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作，有操作日志和维护记录，首自信每月向信息部提交月度总结报告。对于系统漏洞会定期扫描，但是扫描出漏洞后不会轻易进行漏洞修补需要上报信息办审批。《北京首钢冷轧薄板有限公司企业网网络用户管理办法(试行)》中规定“保证所有与外部系统的连接均得到授权和批准;使用安全策略控制移动式设备接入网络”，但是由于目前各基地和总部之间未设置安全域以及访问控制策略，访问时无需认证，无法做到根据业务需求和系统安全来分析安全性；对于重要系统配置及业务数据的备份有定时备份和人工备份两种方式，定时备份一般存在本机或者磁盘阵列上，属于增量备份。人工每月会进行一次磁带备份(全备份，包括数据和配置)，数据备份介质保管在顺义档案室，备份的数据没做过恢复程序；杀毒软件趋势厂家工程师定期对网络和主机进行恶意代码检测并保存检测记录并提交报告；对于系统变更有《信息系统变更管理规定》，由各业务部门向信息办提出更改需求及更改方案，审批通过后，信息办组织相关业务对更改方案进行测试，测试通过后才能上线，如果测试不成功，且短时间无法解决的就把系统恢复；有安全事件的划分，按应急处理时间划分为大体应急、系统类的、

严重类的等，4小时以上没解决的事件属十分严重类型，所有安全事件没有进行过应急演练处理。

(7)工程建设

没有自己的施工队伍，因此采用外部招标方式选择有资质的承建队伍进行施工。办公区域建设与机房建设由不同的单位进行，不想进度受制约。首自信承建机房建设项目，但是由于资源及力量有限，设备采购有采用外部招标由东华公司负责。但首自信公司没有在现场设置项目经理一职，只是根据项目需要的三部分分别设置项目经理，缺少专职协调人。

第4章 首钢冷轧罩退信息系统集成项目风险识别与评估

4.1 首钢冷轧罩退信息系统集成项目风险管理的指导思想

首钢冷轧罩退信息系统集成项目，是由冷轧公司牵头，首自信公司作为项目的总包方，东华公司作为项目的实施方来就行运作的，因此如何合同运作取得最后的双赢是项目管理者应该统筹考虑的。在项目的决策阶段，充分考虑到首钢冷轧公司、首自信公司及城建的东华公司的利益，在工程资料充足及承建单位资质无误的基础上充分考虑建设过程中的各种风险，对建设期进行科学决策。在项目实施和建设阶段，各方应该与企业建设方保持高度一致，提供人员、设备及时，合理运用伙伴关系中的各种集成资源，共同分担、管理各项风险，以达到共赢的结果。项目中建立合作策略，合理配置资源，共同处置风险的指导思想，充分了解项目组织及建设过程中的风险，评估风险影响并及时做出响应，项目的最终目标即按期保质保量的完成才能得以实现。

4.2 首钢冷轧罩退信息系统集成项目的风险因素识别

要想进行有效的风险管理，就需要抓住有效地风险管理因素，忽略不相关的风险，这就需要与项目的管理目标相结合。在针对首钢罩退的信息系统集成项目的特点，首先实施的工作是制定风险计划，见表4.1。

表4.1 计划检查表

Table 4.1 Planning Checklist

检查场所	工作内容
工程现场	漏洞扫描，完成20余台服务器设备的漏洞扫描，完成40台网络设备的漏洞扫描，完成4个网段的办公终端电脑的扫描。
	主机人工审计，完成MES系统、办公系统共20余台服务器设备的主机人工审计。
办公室	应用系统调研，分别对MES系统、OA系统应用现状情况进行调研，完成各应用系统《等保技术要求》、《技术安全保障状况调查表》、《应用评估》、《终端调查表-办公终端》、《资产赋值说明》以及《物理及网络安全调研》等文档10余份；
	物理和网络调研访谈，对信息机房物理环境，相关网络设备的部署现状进行调研，完成《物理安全》、《网络安全》、《技术安全保障》相关技术访谈工作，形成文档；
	调研管理细节，对冷轧公司的安全管理制度、机构构成、人员情况以及系统建设和运维管理层面对相关管理制度及现状进行调研。

风险管理首先进行的是风险识别。风险识别的主要内容是，运用专用工具系统来全

面的识别能够引起项目风险产生的主要因素、各个风险的性质、各个风险可能引起的主要后果。风险的存在可能导致系统受到危害，导致项目建设过程中发生事故的。风险不是虚无飘渺的，而是客观存在的，无论多么坚固的堡垒都是可以突破的就是这个道理。也正是因为风险的存在，组织建设过程的风险识别就想的更为重要，只有充分了解情况，才能够进行正确的判断。整个风险的识别评估阶段，需要全面、准确地去了解系统所面临的各种风险。在评估过程中，评估实施小组与首钢的相关人员对该项目面临的信息安全风险进行了梳理和分析。表4.2列对项目中的风险级别进行了赋值。

表4.2 安全级别赋值表

Table 4.2 Security level assignment table

等级	标识	描述
5	很高	其风险发生可能会对项目造成的后果非常严重，非常重要
4	高	其风险发生可能会对项目造成的后果比较严重，重要
3	中等	其风险发生可能会对项目造成的后果中等，比较重要
2	低	其风险发生可能会对项目造成的后果损失较低，不太重要
1	很低	其风险发生可能会对项目造成的后果损失微小，不重要，甚至忽略不计

项目评估的核心是对安全风险的识别、计算与分析，是对各种评估要素进行综合、关联分析的过程。表4.3列出了项目中各种风险发生的可能性和严重程度。主要分为两部分工作：一部分是各种风险要素的综合关联计算，得出项目相关部分的安全风险值；另一部分工作是对各项目相关风险值进行综合分析，得出业务系统的安全风险值，并对该值进行等级划分，形成易于用户理解的风险等级表述。本结果将会对评估项目的最终评估结论起着关键主导性作用。管理风险主要看是否设立相应的管理机构，在管理机构中是否制定了安全管理制度，对人员安全和系统建设、系统运维进行管理。

项目风险进度主要由于设备到位不及时，设备、材料质量问题等因素引起的。由于工程人员经验不足或者沟通问题，有可能会导致采购的物料或设备与要求存在偏差或者直接不符合要求。而供货商需要一定的供货时间，尤其是进口的物料，出现差错不能马上进行更换，会耽误并拖延整个项目的进度，这类全局风险的存在，要求在整个生命周期内要全局考虑，减少这些风险对项目整体进度的影响，保证上线工作不延误。

表 4.3 项目风险清单

Table 4.3 List of project risks

分类	编号	风险名称	所含风险因素	可能性	严重程度
环境风险	11	自然环境风险	雷电、地震、水灾等	10%	高
	12	机房环境缺陷	由温度、湿度、灰尘引起故障	10%	中
	13	电力故障	主要是电力中断，用电波动，供电设备损坏	20%	高
不可控风险	21	设备硬件故障	计算机设备的 CPU、电源、硬盘、内存故障	20%	低
	22	软件故障	应用软件、数据库软件本身故障	20%	低
	23	恶意代码和病毒	意外事件造成感染木马、病毒、蠕虫等	50%	高
	24	误操作	用户无意执行了错误的操作	10%	中
外部风险	31	远程攻击	为窃取秘密或破坏系统而实施的远程攻击	10%	高
	32	植入恶意代码	黑客、政治间谍为窃取秘密或进一步发起攻击而恶意植入木马	10%	高
	33	篡改或盗取数据	对生产数据进行篡改或为进一步破坏生产而盗取重要信息	20%	高
	34	第三方风险	第三方人员对系统进行非法/非授权操作	50%	高
	35	恶意破坏系统设施	对系统设备、存储介质恶意破坏，盗窃机房设备与设施	10%	高
	36	社会工程	外部人员通过社会工程方式获得敏感数据	20%	中
内部风险	41	非法使用软件	使用未经许可的软件	40%	中
	42	违反授权原则	内部人员使用所授权限进行不正当操作	20%	中
	43	未授权扫描	内部人员未授权的对系统网络、主机进行扫描	50%	高
	44	未授权连接 Internet	使用未授权方式连接 Internet	10%	中
	45	内容人员泄密	内部人员将系统敏感信息泄露给外部人员	20%	高
全局风险	51	进度风险	公司内部对该项目缺少合作	20%	低
	52		项目早期阶段无法准确识别项目风险因素	50%	高
	53		项目经理经验不足或没有专人负责该项目	80%	高
	54		设备交货延期	80%	高
	55		到货的设备有问题需要更换	20%	中
	56		预计外工作影响	20%	中

表 4.3 是影响项目进度风险分析评估表，从中可以看到有三个重要风险因素影响到项目进度，包括早期不能准确识别项目风险因素、项目经理经验不足或没有专人负责该项目、设备交货延期。其中项目经理经验不足和设备延期交货的发生性较高，该工程交由首自信和东华公司共同负责，其人员的水平和能力没有实际工作的检验，都可能造成延误工期的危险因素。

4.3 首钢冷轧罩退信息系统集成项目风险的分析与评估

风险评估建立在风险识别完成后，对风险发生的可能性的分析上。依据风险赋值表，将风险点进行加权赋值，综合考虑风险意图和风险能力等因素，等级赋值越高风险发生的可能性越大。根据所对应风险的客观存在性，某些风险的种类和大小是固定的，而前面划分也是根据风险相同的原则来的。

风险的等级主要是根据经验积累或类似行业的历史数据来确定的。对于那些经验和历史数据中没出现过的风险因素，将主要根据风险的吸引力、风险的技术力量、脆弱性被利用的难易程度等制定了一套标准对应表，以保证风险等级赋值的有效性和一致性。根据固定的赋值准则，分别对不同风险进行了确定。下表中列出的风险均存在发生的可能性，其中不同的等级代表这个风险发生的可能性大小即为该组中所有资产所面临风险的等级。

为科学有效的衡量风险的严重程度，本次信息安全风险评估风险分析采用表4.4风险矩阵计算风险的严重程度：

表4.4 风险矩阵

Table 4.4 Risk Matrix

严重程度 / 可能性	很低(1)	低(2)	中(3)	高(4)	很高(5)
很高(5)	中(3)	中(3)	高(4)	高(4)	很高(5)
高(4)	低(2)	中(3)	中(3)	高(4)	高(4)
中(3)	低(2)	低(2)	中(3)	中(3)	高(4)
低(2)	很低(1)	低(2)	低(2)	中(3)	中(3)
很低(1)	很低(1)	很低(1)	低(2)	低(2)	中(3)

通过对表4.3中项目进行的风险评估，可以清楚地看出评估范围内的业务系统及所面临的风险种类和每种风险发生的可能性。根据综合分析，从风险的三个组成方面，主体、客体以及发生的可能性，对项目所面临的各种风险进行简单描述。

(1)恶意代码和病毒

这种风险的主体为合法及非法用户，主要是合法用户在不知情的情况下运行未知、未经过安全测试的程序造成，风险的客体为软件资产和数据资产。非法用户能够利用系统漏洞和安装恶意代码使系统感染病毒，这种风险发生的可能性由系统的防护体系建设有关，发生的可能性适中。

(2)非法使用软件

这种风险是非故意行为，系统管理员用户或其他合法用户对软件资产或数据资产的等应用程序使用不当时会发生，因此这种风险发生的可能性根据不同的用户(主体)和不同的资产(客体)而不同，一般发生可能性适中。

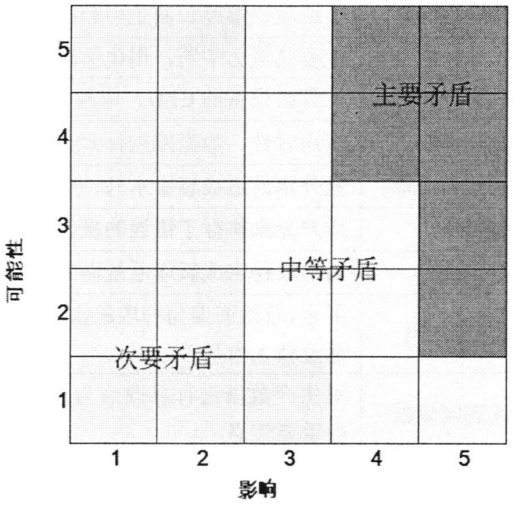

图 4.1 风险矩阵
Fig. 4.1 Risk Matrix

(3)违反授权原则

这种风险是合法用户的故意行为，系统管理员用户或其他合法用户对软件资产或数据资产的等在未授权的情况下通过窃听手段窃取系统软件和应用软件的系统数据及敏感的业务数据，这主要与员工的素质有关，也与用户的权限大小和威胁系统的可利用程度有关，一般发生可能性为中。

(4)未授权扫描

这种风险是合法用户的故意行为，统管理员用户或其他合法用户对软件资产或数据资产的等在未授权的情况下通过密码扫描等工具或其他分析手段对系统软件或应用系统的密码进行分析，这主要与员工的素质有关，也与用户的权限大小有关，一般发生可能性为中。

结合表 4.3, 表 4.4 对项目风险进行量化，形成风险赋值表 4.5。

表 4.5 风险赋值表
Table 4.5 Risk assignment table

分类	编号	风险项名称	说明	风险等级
环境风险	11	自然环境风险	雷电、地震、水灾等	2
	12	机房环境缺陷	由温度、湿度、灰尘引起故障	2
	13	电力故障	主要是电力中断，用电波动，供电设备损坏	2
意外风险	21	设备硬件故障	计算机设备的 CPU、电源、硬盘、内存故障	2
	22	软件故障	应用软件、数据库软件本身故障	2
	23	恶意代码和病毒	意外事件造成感染木马、病毒、蠕虫等	3
	24	误操作	用户无意执行了错误的操作	2
外部风险	31	远程攻击	为窃取秘密或破坏系统而实施的远程攻击	2
	32	植入恶意代码	黑客、政治间谍为窃取秘密或进一步发起攻击而恶意植入木马	2
	33	篡改或盗取数据	对生产数据进行篡改或为进一步破坏生产而盗取重要信息	2
	34	第三方风险	第三方人员对系统进行非法/非授权操作	2
	35	恶意破坏系统设施	对系统设备、存储介质恶意破坏，盗窃机房设备与设施	2
	36	社会工程	外部人员通过社会工程方式获得敏感数据	2
内部风险	41	非法使用软件	使用未经许可的软件	3
	42	违反授权原则	内部人员使用所授权限进行不正当操作	3
	43	未授权扫描	内部人员未授权的对系统网络、主机进行扫描	3
	44	未授权连接 Internet	使用未授权方式连接 Internet	2
	45	内部人员泄密	内部人员将系统敏感信息泄露给外部人员	2
全局风险	51	进度风险	公司内部对该项目缺少合作	2
	52		项目早期阶段无法准确识别项目风险因素	4
	53		项目经理经验不足或没有专人负责该项目	4
	54		设备交货延期	4
	55		到货的设备有问题需要更换	3
	56		预计外工作影响	3

4.4 首钢冷轧罩退信息系统集成项目风险的量化分析

4.4.1 首钢冷轧罩退信息系统集成项目风险的量化和计算

(1) 风险量化的计算模型

本评估项目中，采用 GB/T20984-2007《信息安全风险评估规范》[12]中的风险计算模型，表示式如下：

风险值=R(A，T，V)= R(L(T，V)，F(Ia，Va))　　(4-1)

其中，R 表示安全风险计算函数；A 表示系统；T 表示风险；V 表示脆弱性； Ia 表示安全事件所作用的系统价值；Va 表示脆弱性严重程度；L 表示风险利用系统的脆弱性导致安全事件的可能性；F 表示安全事件发生后造成的损失。

在风险的具体计算中，含有以下三个关键计算环节：

计算安全事件发生的可能性

根据风险出现频率及脆弱性的状况，计算风险利用脆弱性导致安全事件发生的可能性，即：安全事件的可能性=L(风险出现频率，脆弱性)＝L(T，V)。

计算安全事件发生后造成的损失

根据系统的价值及脆弱性严重程度，计算安全事件一旦发生后造成的损失，即：安全事件造成的损失=F(系统价值，脆弱性严重程度)＝F(Ia，Va)。

计算风险值

根据计算出的安全事件的可能性以及安全事件造成的损失，计算风险值，即：风险值=R(安全事件的可能性，安全事件造成的损失)＝R(L(T，V)，F(Ia，Va))。

(2) 风险计算方法

在评估项目的过程中，选择用“相乘法”的风险计算方法来计算业务和系统的风险值。具体计算公式为：

安全事件发生的可能性 L=T*V　　(4-2)

安全事件发生后造成的损失 F=V*A　　(4-3)

系统的风险值 Rn=L*F　　(4-4)

业务的风险值 R=Max(Rn)　　(4-5)

4.4.2 安全风险级别分析

安全风险等级划分说明：本次安全风险评估项目中，对信息系统的取值范围界定为“1--5”，风险的赋值范围为“1--3”，脆弱性的取值范围界定为“1--5”。

因此，按照 GB/T20984-2007《信息安全风险评估规范》中的“相乘法”计算分析模型，可得到业务、系统的风险值取值范围为“1--375”。为方便用户对其业务、系统最终风险的理解，将风险值转换为“风险等级”的概念，具体转换参见表 4.7。

表4.6 安全风险计算表

Table 4.6 Security risk calculation table

业务系统	IT资产	最高最弱性问题	脆弱性赋值(V)	风险赋值(T)	系统赋值(A)	安全事件发生的可能性 L(L=V*T)	安全事件产生的损失 F(F=A*V)	系统风险子项值 Rn(Rn=L*F)
MES系统	MES生产系统服务器/备机、测试系统服务器、归档服务器、打印服务器、备份管理机	OpenSSH S/Key 远程信息泄露漏洞	4	3	4	12	16	192
		OpenSSH GSSAPI 信号处理程序中存在安全漏洞	4	3	4	12	16	192
		HP OpenView Storage Data Protector 备份客户端服务溢出漏洞	5	3	4	15	20	300
		格式化串对 statd 的攻击	4	3	4	12	16	192
		Oracle 2010.04 安全更新修复多个安全漏洞	4	3	4	12	16	192
		密码设置策略的口令生存期不符合规范	3	3	4	9	12	108
办公系统	OA服务器、OA数据库服务器、档案服务器邮件服务器	OpenSSH S/Key 远程信息泄露漏洞	4	3	3	12	12	144
		OpenSSH GSSAPI 信号处理程序中存在安全漏洞	4	3	3	12	12	144
		MySQL 空口令	4	3	3	12	12	144
		MySQL Community Server 5.0 < 5.0.67 存在多个漏洞	4	3	3	12	12	144
		密码设置策略的口令生存期不符合规范	3	3	3	9	9	81

表4.7说明首钢顺义冷轧公司应用系统风险等级存在“高风险”系统。其中“MES系统”最高风险值为300，是因为上述应用系统中脆弱性赋值中都包含赋值为5的“很高风险”因素，在分别与风险赋值“3”和资产赋值“4”相乘后得出风险值为300；“OA系统”的脆弱性赋值中存在最高级别风险等级为“4”的“高风险”因素，在分别与风险赋值“3”和资产赋值“3”相乘后得出风险值为144，最后使用加权平均的方法计算后，得出“MES系统”风险值为196；“OA系统”风险值为131，均为“中等”风险。

表 4.7 风险等级表

Table 4.7 Level of risk table

风险值范围	1~55	56~130	131~260	261~335	336~375
风险等级	1	2	3	4	5
等级标识	很低	低	中等	高	很高

表 4.8 业务系统安全风险等级划分

Table 4.8 Business system security risk classification

业务系统	系统资产	风险值	风险等级	等级标识
MES 系统	MES 生产系统服务器/备机、测试系统服务器、归档服务器、打印服务器、备份管理机	196	3	中等
办公系统	OA 服务器、OA 数据库服务器、档案服务器、邮件服务器	131	3	中等

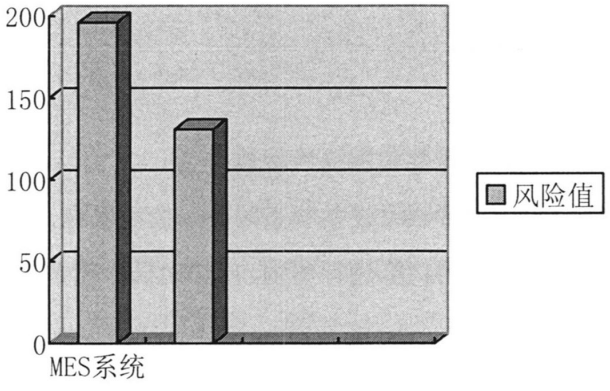

图 4.2 系统风险值统计图

Fig. 4.2 Systemic risk value charts

通过对各类风险评估要素的计算、分析，可以看出，首钢顺义冷轧信息系统的安全状况(表 4.9)为“中风险”：“中等”风险级别所占比例为 100%，风险总体情况为中等。

表 4.9 业务系统安全风险等级统计

Table 4.9 Business systems security risk level statistics

风险等级	1	2	3	4	5
等级标识	很低	低	中等	高	很高
业务系统风险等级数目	0	0	2	0	0
业务系统风险等级百分比（%）	0%	0%	100%	0%	0%

4.5 首钢冷轧罩退信息系统集成项目风险评估中存在的问题

通过对项目风险的评估结果进行研究，发现在项目风险评估的过程中存在值得关注的部分，概括为以下两个方面：

(1)物理建设过程

对于项目中的机房建设，要求按照国家标准做到物理访问的控制、防盗窃的部署、防破坏的能力、防止雷击的装置、防火设备的配置、防水的环境搭建和防潮能力、防静电环境、温湿度的控制、电力供应保障和电磁防护。目前项目评估中发现基本按照这些要求在进行，但是由于物理位置和工程建设款的短缺，部分没完全达到设计要求。

①机房门使用的是传统的机械锁，没有按照要求在机房配置电子门禁系统，控制、鉴别和记录进入人员。

②机房内没有采取区域隔离防火措施，将重要设备与其他设备隔离开。

③机房内有窗户，未进行封闭，没有采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。

(2)网络系统安全

①没有限制网络最大流量数和网络连接数。

②没有在网络系统中设置网络设备状态的同一监测平台，采用的逐一上机查看。

③主要网络设备目前只用口令进行鉴别，应该对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别。

第5章 首钢冷轧罩退信息系统集成项目风险监控与应对

5.1 首钢冷轧罩退信息系统集成项目风险控制的目标

企业信息化项目的集成风险管理，在风险监控过程中,应该定期组织项目的相关人员进行关于项目相关事项的有效沟通,将监控作用到项目的全生命周期中，并对企业信息化项目中的风险水平的可接受程度不断地进行重新评估。将风险监控提供的相关信息,用于风险再次发生前的有效决策，不断充实，不断改进,对风险进行有效防范。

首钢冷轧信息系统网络架构风险是通过对网络拓扑结构及基本安全策略的调研与分析，以及对网络设备进行安全漏洞扫描等方式，分析出设备及网络安全策略中存在的风险，因此针对目前系统确立风险控制的目标：

(1)物理安全

物理安全建议依据《信息系统安全等级保护基本要求》(GB/T22239-2008)三级物理安全要求，通过物理位置的选择、物理访问的控制、防盗窃的部署、防破坏的能力、防止雷击的装置、防火设备的配置、防水的环境搭建和防潮能力、防静电环境、温湿度的控制、电力供应保障和电磁防护这十个安全控制点进行检查，列出目前信息机房存在的安全隐患，并提出安全加固建议，其中标注“等保三级要求”的项是为满足等级保护三级的要求而提出的，其余各项均为等级保护二级要求，在整改过程中可根据企业情况，逐步完善。

应对机房划分区域进行管理,区域和区域之间设置物理隔离装置;例如网络设备区、服务器区、供电设备区使用玻璃隔断或者金属网进行物理隔离；应利用光、电等技术设置机房防盗报警系统；机房空调设有加湿装置，水管从地板下通过，水管应重新进行防护，防止漏水现象的发生；应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透，目前机房窗户应该进行彻底封闭，并密封加固；机房配置了海洛斯精密空调机组，能够自动调节温度与湿度，使用上出风设计，机房内温度控制不均匀，目前温度25度左右，应设置通风设备，使机房内各个区域温度相同；应采取措施防止机房内水蒸气结露和地下积水的转移与渗透，应设置机房环境监测系统，设置水感器件，对机房进行防水检测和报警(等保三级要求)；应建立备用供电系统，配备柴油发电机，或者设置可接驳移动发电设备的电力接口(等保三级要求)。

(2)网络架构安全

应将不同安全级别的应用系统按照功能划分在不同的安全域，如数据库服务器应该与不同的应用服务器、DMZ 区等实现安全域隔离、各业务应用服务器与办公终端实现安全隔离、不同的远程接入区域之间实现安全域隔离等；安全域隔离方式可采用 VLAN 方式，也可采用网闸方式等。

核心部分设备和链路都有冗余设计，互联网与专线接入区链路及网络设备存在单点故障隐患；例如：负责互联网与专线接入的一台 Cisco3560 设备存在单点故障隐患，应将该网络设备进行冗余结构部署，保证互联网与专线连接的可靠性；目前在网络边界只部署少量访问控制设备，只在互联网出口处部署，在专线连接的专线边界未时用安全设备，会导致无法控制来自其他地区的非法访问； 应在互联网边界部署性能良好的安全设备，在与各地连接的专线边界部署安全设备；整体网络架构中安全防护能力较弱，建议从网络边界保护、网络安全域保护、网络访问控制及网络审计四个不同层面进行网络整体防护能力的提升；在网络访问控制方面，需要在路由器、交换机、防火墙、网闸等设备上实施严格的访问控制策略，严格控制端口与 IP 地址的访问；对于 Web 应用，需要部署 Web 防护系统等，从应用层面加强网络系统的防护。对于网络审计，需要增加集中审计系统、流量监测系统等，实现对各网络设备、安全设备等系统的集中审计与网络流量异常的监控，及时掌握各设备的运行状况与网络流量的状况。

(3)应用系统安全

在应用系统的建设中，目前网络中没有划分安全域，所以无法有效地进行 ACL 及其他安全策略的配置和部署；终端用户到各应用系统之间的访问控制较少，例如在顺义冷轧办公楼的办公区接入网络后，均能够对所有应用系统服务器进行访问，没有明确的访问控制范围。应该在业务终端与业务服务器之间进行路由控制建立安全的访问路径；按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机；目前对带宽的限制只是对于上互联网的员工终端通过计费网关进行控制，其它并没有严格限制。核心部分设备和链路都有冗余设计，互联网与专线接入区链路及网络设备存在单点故障隐患；例如：负责互联网与专线接入的一台 Cisco3560 设备存在单点故障隐患。

在网络边界部署访问控制设备，启用访问控制功能；目前只有在互联网出口处部署防火墙设备，防火墙配置了访问控制策略及 NAT 配置，到北京总部的专线连接处没有设置安全设备。对登录网络设备的用户进行身份鉴别，目前使用用户名密码登录，但未进行级别划分，多管理员公用一个用户名密码，设置了 console 和 telnet 的登录口令。

对网络设备的管理员登录地址进行限制，目前未做限制。主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别，目前只使用用户名密码进行鉴别。身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换，目前复杂度没有要求，且没有定期更换密码。实现设备特权用户的权限分离，目前未进行级别划分。

5.2 首钢冷轧罩退信息系统集成项目风险应对的措施

首钢企业信息系统的安全防护要贯彻国家有关信息安全防护政策，信息系统的安全防护除了要考虑系统的安全部署外还要在安全的成本投入和风险防范之间进行平衡，对网络及信息系统安全配置进行合理的优化，分等级对网络和信息系统进行保护，以确保与生产运行相关联的、和公司利益关系较大的信息系统安全。

5.2.1 总体安全策略

信息安全的部署策略是首钢的信息安全工作遵循的基本依据。根据公司特点和安全需求，总体安全策略分成四部分：

(1)系统分级

根据业务应用系统、业务应用子系统(业务应用系统模块)的使命、目标以及重要程度，对系统进行安全等级的划分。

(2)防护分域

网络安全域是一个包含单个或多个业务系统的网络防护区域。安全域具有等级属性，安全域的等级同其内部的业务系统等级相同。

防护分域是指根据网络安全域内的业务系统定级情况和业务系统的服务对象，针对不同安全域采取不同强度的安全防护措施。

(3)预防为主

信息安全防护应以预防为主，就是要把预防信息安全事故作为防护的出发点和落脚点，从信息安全风险管理的角度、信息系统全生命周期各阶段的特点、业务系统的安全特性出发，有组织、有计划地采取主动、严密的预防措施，达到防患于未然的目的。

(4)积极管控

由于信息安全事件具有动态变化、突然爆发、持续破坏、高度不可预测等特性，因此为了全面应对信息安全事件需要建立积极的管控机制，融合技术和管理手段，实现对

信息安全风险的主动跟踪、及时掌握、有效处理，达到可控、能控、在控的管理效果。

5.2.2 总体框架

将各系统划分安全域进行防护，将各安全域划分为网络边界、网络环境、主机系统和应用环境四个层次实施安全措施防护。

5.2.3 防护原则

基于安全防护体系建设的长期性和复杂性，在安全分区的基础上，遵循以下总体安全防护原则进行信息系统安全防护体系建设。

(1)分区分域：将首钢信息系统进行进一步的安全域划分，以实现不同安全等级、业务类型系统的独立化防护、差异化防护。

(2)等级防护：信息系统将以实现等级保护为基本出发点进行安全防护体系建设，依据系统定级情况进行安全域划分，并参照国家等级保护基本要求进行安全防护措施设计。

(3)多层防御：在分域防护的基础上，将各安全域的信息系统划分为边界、网络、主机、应用四个层次进行安全防护体系设计，以体现层层递进，逐级深入的安全防护理念。

5.3 首钢冷轧罩退信息系统集成项目风险应对

根据项目风险的基本特征和风险决策的基本原理，想要对本项目的全面风险进行有效的管理，需要关注以下内容：

(1)健全安全管理机构

建议尽快成立专门的信息安全管理组织机构(该机构的人员组成中应由信息化主管领导担任领导职务)，抓紧制定和完善首钢信息安全管理制度与规范，并下发相关各单位严格执行；明确安全管理机构各个部门和岗位的职责、分工，明确技能要求；保证专人专岗，目前信息系统的保密性和安全性较差，特别是关键岗位，需要行驶职责分离机制，保护关键业务的安全。

(2)加强人员安全管理

对于普遍存在的人员信息安全培训不足的问题，建议加强各单位信息化部门、各系

统运维管理人员、系统使用相关人员等的信息安全培训，提高相关业务人员的安全意识，增强 IT 技术人员的安全技能；对于内部人员迄今为止还未签署岗位安全协议的问题，建议首钢信息安全主管部门会同人事部门，积极推进岗位安全协议的签订，共同加强内部人员的安全管理；信息安全培训工作需要分层次、分阶段、循序渐进地进行，而且必须是能够覆盖全员的培训；分层次培训是指对不同层次的人员，如对管理层(包括决策层)、信息安全管理人员，系统管理员和普通员工开展有针对性和不同侧重点的培训；分阶段是指在信息安全管理体系的建立、实施和保持的不同阶段，培训工作要有计划地分步实施。

(3)强化系统运维管理

建议加强对厂商、首自信等第三方运维服务的管理，通过运维制度建设、运维管理规范化、合同约束等方式对可能由第三方运维服务引起的安全风险进行防范；所有网络必须具有关于拓扑结构、所用设备、链路使用情况等关于网络情况的详细说明文档，并保持文档内容和现有网络、设备连接和链路信息保持一致。

(4)建立并完善安全管理制度

对于本次评估项目中反映出的安全管理制度缺乏的问题，建议首钢信息部要着手加强制定相应的运维操作规程、建立相应的日常管理操作规程，并在实践工作中进行应用。

(5)加强业务连续性管理

对于普遍存在应急预案缺失的问题，建议信息安全主管部门尽快组织技术力量，加紧制定涉及各主要业务系统的安全应急预案，至少应包括电力中断、病毒爆发、网络中断、业务系统瘫痪、自然环境突发事件等可预见性事件的预案，并定期对应急预案进行演练、总结和完善；目前重要应用系统都采用双机形式，可进行互备，但没有灾备系统；重要数据每天备份，采用磁带进行备份，备份介质主要存放于本地，定期把重要数据存放到档案馆，非重要数据本地存储；应建立基于网络的实时灾备系统，或者加强备份工作的执行，严格按照备份实施计划执行，并定期举行恢复演练。

5.4 首钢冷轧罩退信息系统集成项目风险应对反馈

2012 年 5 月 1 日首钢冷轧罩退信息系统集成项目正式上线，比计划提前一个月时间，目前正在试运行阶段。在项目建设期，运用项目风险管理理论和工具对项目进行了全面管理。对于项目来说，成本、质量和时间是最为重要的控制点，而对于本项目来说，保证系统能够在规定时间内完成并顺利上线运行，整个系统通讯正常，是首钢冷轧提高

管理和降低成本的基础。

项目过程中按照风险评估结果和管理思路，调整项目架构，降低风险点，为项目的提前完工上线起到了保障，有效地节约了运营成本，保障了工程质量，为项目的正常运行打下了基础。

第6章 结论与展望

6.1 论文结论

信息系统项目风险管理对于项目目标的实现是非常重要的，但目前仍然算是一门新兴的边缘学科，在国外的到了飞速的发展，而我国却起步较晚，尚处于研究和应用的初步阶段。对于工程项目而言，进行完善的风险管理是非常重要的，不但可以提高项目的成功率而且可以增强项目的积极性和投产后的竞争力。风险管理对于项目目标的实现是非常重要的，但目前风险管理研究大多专注于对风险管理具体方法和技术的研究，另外，由于项目参与方众多，各方从自身的角度进行风险管理，是项目分享管理处于分割与分散性状态。企业信息化的快速稳定发展对于我国工业化进程的顺利进行具有重要意义，制造业信息化是提升我国制造业竞争力和综合国力的重要手段。信息系统的应用与实施是当前我国制造业信息化的重要内容之一。但是现在信息系统在我国制造企业的应用状况是实施的成功率较低，造成这种状况的主要原因是我国制造企业的管理模式与信息系统所蕴含的管理模式不相符，信息系统管理与企业经营管理之间存在较大的差距。

本文通过对首钢冷轧罩退信息化系统集成项目所蕴含的风险进行了系统的风险研究，利用风险管理理论和分析评估方法，对各项风险进行了识别、评估，提出了相应的风险控制措施。其主要研究结论如下：

(1)通过对项目的风险进行识别，结合项目的自身特点，归纳总结后提出了项目中物理设备建设、网络环境部署、应用系统开发三个重要过程的风险因素，并对这些因素进行分析，得出其产生的根源、条件。

(2)通过对项目中存在的每个风险的评估，将项目中所涉及的风险整合到项目的战略规划、项目的整个实施活动和角色过程中，对项目的风险进行分析和量化，对在对项目风险进行识别的基础上，确定该项目风险发生的可能性及其影响程度，得出风险管理和控制措施制定的依据。

(3)通过对首钢冷轧罩退信息系统集成项目的风险管理研究，得出在信息系统集成项目中以整体结果最优为目标进行风险分析、评估、防范风险发生的安全配置策略和防护原则的结论。

项目的风险是客观存在的，不可避免的，但是作为管理者要采用积极的态度去面对风险。利用项目风险管理环将项目风险管理的四个过程进行集成，并在此基础上，同项

目管理过程和项目全寿命周期进行了集成。将项目风险管理各阶段方法的优点、缺点和适用范围进行了汇总分析。

6.2 进一步展望

随着时间的推移、经济的发展、技术的进步、项目管理思想的日趋完善，系统集成项目的风险管理也在动态的变化，项目规模日益扩大，实现难度日益增加，这些都给集成项目的风险管理研究带来了巨大的挑战。项目的集成化对管理团队的水平提出了很高的要求，因此提高人员素质也成为项目管理成败的重要部分。同时，成熟的集成风险管理体系研究将更好的推动和促进整个项目管理理论的完善和发展，因此建立完善的管理模型的将成为该领域未来的重要发展方向。

参考文献

1. 谢绪丽. 从风险管理视角谈内部审计[J]，黑龙江对外经贸，2009(04).
2. 戚安邦. 项目管理十大风险[M]，北京：中国经济出版社，2004，102-1.
3. 陈应田. 浅谈工程项目管理的现状及应对策略[J]，魅力中国，2011(12).
4. 谢喜丽. 项目风险管理发展历程及趋势[J], 合作经济与科技，2010(14).
5. Hau Lee, Mitigating supply chain risk through improved confidence[J].International Journal of Physical Distribution & Logistics Management,2004,34(5):388-396.
6. 刘晓红. 徐玖平. 项目风险管理[M]，经济管理出版社, 2008.
7. 毛晓东. 系统集成项目管理的步骤与分析[J]，江苏科技信息, 2009(9).
8. 夏胜权. 基于综合集成研讨厅的工程项目集成风险管理研究[J]，科技信息, 2009(25).
9. 张毅. 石油工程项目风险管理研究[J]，中国西部科技，2011, 10(13).
10. 姜学龄. 刍议水利水电项目风险管理理论[J]，建材与装饰：上旬. 市场营销，2010(04).
11. 张凯. 工程项目风险管理浅析[J]，经济师，2009(05).
12. 柳纯录. 信息系统项目管理师教程[M]，北京:清华大学出版社, 2008.
13. 李勘. 武器装备研制项目集成风险管理研究[J]，科学学研究，2010.
14. 郭波等编著. 项目风险管理[M]，电子工业出版社, 2008.
15. 李然. 浅谈建设工程项目管理[J], 中国新技术新产品，2010(14).
16. 刘汕. 张鑫隆. 陈涛. 丛国栋. 企业 IT 项目风险评估与规避策略研究[J]，管理学报，2009(04)：224-270.
17. 袁智伟. 论信息系统集成项目中的风险管理[J]，中国市场, 2010(45)：62-80.
18. 晓芳. 郝建君. 高新技术企业全面风险管理实施框架——基于美国 COSO 企业风险管理框架[J]，科学管理研究，2010(02).
19. 冯社洪. 浅析科研活动的风险管理[J]，经济师，2011(10).
20. 何静. 系统集成项目中的风险管理[J]，吉林师范大学学报（自然科学版），2010，38(1)：106-110.

21. 钱巍. 浅析企业全面风险管理与 IT 项目风险管理的关系[J]，项目管理技术，2009(S1).
22. 王慎丽. 道路桥梁施工中工程项目管理浅谈[J]，建材与装饰下旬，2011(04).
23. 安静. 浅析工程项目风险分析与评价[J], 中国经贸导刊, 2009(15).
24. 白剑峰. 工程项目 PFI 模式风险识别技术[J]，科学创新导报，2010(35).
25. 杨小舟. 企业全面预算的风险管理[J]，财务与会计, 2009, 7:46-48.
26. 尤荻. TOT 项目风险集成管理模式研究[J]，项目管理技术，2011(1).
27. 汤成. 基于伙伴关系的工程项目风险管理[J]，经济研究导刊，2011(16).
28. 詹簪. 浅谈 IT 项目管理[J]，机械与电子科技信息，2011，25(11)，476-485.
29. 陈建斌. 武刚. 路梅. IT 项目风险管理关键成功因素实施分析[J]，安徽农业科技，2010，45(38)，273-276.
30. 阎广华. 燃气信息化项目风险管理分析与研究[J]，城市公用事业，2009(01).
31. 孙波. 项目风险管理的成熟度模型研究[J]，现代商业，2010，35(32)：65-74.
32. Lambert, Douglas M. Supply Chain Management: Processes, Partnerships,Performance. 3rd Edition[M]. McGraw-Hill, 2008.
33. Sushil Paigankar. How successful Organizations Align Business with IT Using IT Portfolio Management and an IT Governance for Framework [J], Align Journal, 2008, 33(04).
34. 宁定宇. 公路工程项目风险管理初探[J], 黑龙江科技信息，2011(02).
35. 钟侑. 浅论我国建筑施工企业风险管理研究及现状[J], 科学之友：C 版，2009(10).
36. 【美】戴维•克利兰著，杨爱华等译. 项目管理战略设计与实施[M]，机械工业出版社，2002.
37. 刘晓红. 徐玖平. 项目风险管理[M]，经济管理出版社, 2008.
38. 朱勇. 信息系统集成项目管理实践浅析[J]，消费导刊, 2009(18).
39. 乞建勋, 张丽英. 刘严. 杨尚东. 企业全面风险管理的理论与实践梳理[J]，中国市场，2009(18).
40. 王进. 系统集成项目的风险管理应用[J]，中国科技信息，2010，10（3）：90-91.

致谢

在论文结尾之际，谨向所有对我学习和论文撰写过程中提供帮助和支持的人表示衷心的感谢。

首先，本文的研究工作是我的导师张吉善副教授悉心指导下完成的，从选题到论文撰写完成，张老师严谨认真的治学态度、渊博的专业知识使我受益终生。他帮助我很好地实现了理论研究与实际工作的结合，在论文完成之际，谨向张老师表示深深的敬意和诚挚的感谢！

其次，在攻读硕士学位期间，东北大学任课老师及班主任宋老师都在工作、学习等方面给予了我无私的帮助，此外在本课题的研究和论文的撰写过程中，得到了许多同事和朋友们的热心帮助和支持，在此表示感谢。

页　　数：41

字　　数：30660

图：　6

表：　10

参考文献：40