最新光谷一路电力改造 电力系统安全运行与技术改造研究论文(优秀5篇)

在日常的学习、工作、生活中，肯定对各类范文都很熟悉吧。相信许多人会觉得范文很难写？以下是我为大家搜集的优质范文，仅供参考，一起来看看吧

光谷一路电力改造篇一

要提升电力系统的安全运行效率，就需要做到以下几个方面，即：首先，应该建立电力系统运行部门，建立健全的制度。为了能够确保电力系统运行能够有效的管理，相应的供电单位可以设立相应的配电运检组，负责电力系统的运行和维护工作。同时，运检小组还需要在整个工作的过程中严格的检修供电线路，不断的进行巡视和检修工作。为了能够提升运检小组的工作效率与质量，需要对其工作人员进行严格的培训，提升其综合素质。成立运检小组能够缓解配电管理工作人员的工作压力，减少工作人员的任务量，同时还能够有效的避免由于区域之间存在的差异，给配电管理带来消极影响。另外，运检小组的成立能够及时的发现电力系统中的问题，以有效的解决其问题。最后，在改造电力系统的过程中，应该本着“小容量、密布点、短半径”的基本原则。在近几年变电站发展中，已经发生了很多由于变电站超负荷而导致线路烧毁问题的出现。这些事故的发生明确表示，仅仅增加变压器的容量是不可能将电力系统中存在的问题从根本上解决的。只有应用新建台区的方式来分开负荷的分布，将供电变径缩短，有效的缩减损耗，才能够有效的提升电力系统在运行中的安全性，并且确保运行的效率。

4总结

本文主要从三个方面分析了电力系统的运行现状、改造电力系统应该坚持的原则以及电力系统的运行管理与技术改造。

从分析中明确了当前我国电力系统维护与技术改造中还有很多不足存在，这些不足不仅影响着电力系统运行效率，还给我国电网企业的发展带来一定的冲击。为此，要提升电力系统运行效率，提升电力系统改造技术效率，就需要做好维护与管理电力系统的工作，如提升管理力度等等，从而为整体电力系统的运行创建良好的条件。

参考文献

光谷一路电力改造篇二

电子档案管理系统作为电子政务系统中相对独立的子系统，发挥着承前启后的重要作用。它既要维护归档文件的原始性，也要保障所移交档案的可读性，这一定位决定了它具有不同于其他信息系统的安全需求。电子档案管理系统接收归档文件后，集中化的档案资源存量及其利用权限都有所改变，需要对具有复杂来源的档案进行真实性和长期性管理。面对归档、移交的流程需求，如何在异构环境中维持并兼顾档案安全与档案管理的连续性，是本刊连载电子政务系统中档案安全保障的基本问题。因此，只着眼于一般意义上的信息安全保障体系来探讨电子档案的安全保障问题，显然缺乏针对性。应该结合档案工作实际和管理流程，面向保管和利用，明晰安全需求，提出切实可行的安全保障措施。

1电子档案安全保障的主要内容

1.1电子档案安全保障的范畴

信息安全理论体系为电子档案安全保障搭建了技术视角的基本框架，但从实践情况看来，现有的安全保障体系还需与档案管理流程深度结合，否则，电子档案安全保障的特有需求容易被模糊和忽略。综观目前电子档案安全保障的相关研究，较为流行的观点是将电子档案安全目标归纳为保障信息的真实性、机密性、完整性和可用性，［1-2］以及可追究性、不

可否认性、可控性［3］等。从根本上而言，在信息安全的大背景下，上述目标往往是共性的要求。不仅是档案管理系统，所有业务系统如办公自动化系统、人事管理系统、财务管理系统等，都以维护上述属性作为基本的安全保障目标。从流程上看，电子档案管理系统具有特殊的管理定位与职责权限，除基础性安全保障以外，它还具有不同于其他业务系统的安全需求，这些特殊的专业性需求是档案界应予关注的重点。因此，我们认为，除了要关注共性要求之外，更关键的是要结合档案管理的特点和需求来探讨电子档案的安全保障问题。应当根据电子档案管理过程中的不同职能，有所侧重地明晰安全需求，赋予电子档案安全保障更加具体的内涵。在纸质档案管理中，一般将安全管理分为实体安全与信息安全。但由于档案信息内容与纸质载体相对稳定合一，档案实体安全实际表现为档案载体安全，二者在实践中几乎是等同的；信息安全在一定程度上依赖于载体安全。因此，对于纸质档案而言，安全保障通常以档案载体安全管理为主，载体管理在很大程度上决定了档案的信息安全。电子档案信息内容与物理载体的可分离性，导致档案信息安全的管理需求较之以往有所不同，档案实体安全也不再等同于物理载体安全。对于电子档案安全管理而言，可以更为明确地区分出信息安全、实体安全和载体安全三个层面。其中，信息安全主要针对电子档案的信息内容而言，指电子档案内容不被泄露或违规扩散；实体安全主要指电子档案实体（包括电子档案及其元数据、凭证信息等）不被丢失、删改、损坏而导致不可读、不可用；载体安全则主要指电子档案存储载体和软硬件系统等运行环境稳定、存续，不被盗取、破坏，可以支持电子档案存储和读取。载体安全是实体安全和信息安全的基础前提，如果载体遭到破坏，也意味着档案实体会遭到损坏，信息安全则更无从谈起；但仅仅保障载体安全，并不等同于档案实体和信息内容得到妥善管理。比如，在电子档案管理系统运行良好的情况下，也会因人为误操作而删除电子档案，导致电子档案实体丢失；又或是在电子档案实体未遭损坏的情况下，档案信息内容被非法访问和拷贝，导致电子档案信息内容泄漏。因此，信息安全以实体安全为前提，实体安全又以

载体安全为前提，电子档案管理应对三个层面的安全都予以重视。具体而言，无论是纸质档案还是电子档案管理，档案部门对于档案载体安全的管理主要都是通过制定保存管理策略来弥补技术本身固有的局限。因为载体的寿命在客观上是由技术发展的程度决定的，档案部门无法决定文件形成部门选用何种载体存储文件，档案部门的主要责任在于文件归档后为其提供稳定、防磁的库房环境，做好防盗、防损工作，并结合长期保存需求，选择适宜的载体与技术实施复制迁移。对于电子档案的信息安全与实体安全而言，其保障管理需求则有所不同。在信息安全方面，由于数字化信息内容易于复制和传播，对电子档案信息内容的利用控制不再依赖于载体安全来实现，相对于纸质条件而言具有更加独立的安全要求，因此需要在档案利用过程中加以控制。在实体安全方面，在档案保管过程中是对电子档案实体的真实性和长期可读性进行管理；在档案利用过程中则是维护电子档案原件的实体安全。据此，基于档案管理流程与需求的视角，我们将以档案保管和利用两个档案管理流程中的不同阶段为框架，将电子政务系统中的档案安全保障置于这一框架中，结合档案管理理论与实际的要求，对电子档案安全保障的管理策略与技术措施进行梳理与分析。

1.2理论层面的关注

电子档案安全保障实践面临许多亟待解决的问题，这些问题依赖于理论研究发挥更好的指导作用。从电子档案安全保障的影响因素看，首先，技术状况对电子档案安全具有很大影响，例如软硬件漏洞、病毒风险、嘿客攻击、设备与系统风险等都会造成电子档案信息的损坏与丢失。其次，自然因素与社会因素共同影响着电子档案的安全，例如保管场所的条件、天灾人祸等因素。再次，一些管理问题如管理规范缺失、管理权限混乱、管理人员疏漏等都危及着电子档案的安全。［4］由于电子档案安全受到多重因素的影响，电子档案安全保障需立足全方位进行规划与统筹。对此，许多学者提出从实体安全、软件安全、信息内容安全以及网络安全等多方面

着手，［5］提倡通过建立安全保障体系来保障电子档案信息的安全性、完整性和可用性。［6-9］具体而言，包括对技术、管理与法规三方面进行完善。在技术方面，主要提倡自主研发管理系统，对归档电子档案采取杀毒、加密、隔离、备份等技术性保障措施；在管理方面，强调增强管理人员安全意识，完善管理与监督机制，加强专业人员培养等；在法规方面，要求从法律层面明确电子档案的凭证性，不断完善法规标准，以实现电子档案安全管理规范化。一些学者将整个安全体系分为应用层、系统层、网络层、物理层、管理层，根据不同层的安全需求提供管理与技术保障，以构建多层次的安全保障体系。［10］以信息安全的共性规律为基础，在应用于不同领域的安全保障体系之间，同一层次大体上都采取相同的安全保障措施。对于档案安全而言，还需进一步与实际需求紧密结合，才能构建与档案管理相契合的安全保障体系。除此之外，另一种视角是通过风险管理完善电子档案的安全保障。［11-12］信息的风险管理强调对信息系统生命周期的全过程管理，包括完整的风险管理过程：风险管理计划的制定、风险识别、风险评估、风险应对、风险监控，从不同方面采取相应措施以应对可能发生的风险。从宏观上看，目前我国不同地区、不同单位的电子政务建设水平参差不齐，远未达到一体化、平均化的建设效果，具体的风险评估与管理需要因地制宜地规划和实施。从微观上看，基于风险管理的电子档案安全保障要求构建一个体系化的实施方案，风险的多样性和动态性也要求档案人员更加全面地掌握广泛的管理、技术、法规知识，总体的实现要求较高。因此，要达到理想的实践效果，还需结合实际进一步研究。主要从信息安全保障体系和风险管理视角出发的现有电子档案安全保障研究及其成果，已经在事实上为进一步深化研究奠定了一定的基础。为了更好地适应我国电子政务环境下的档案信息化实际情况，有必要从档案管理的视角出发，立足于档案管理流程以及档案部门的职责与实际要求，对电子档案安全保障需求进行梳理与分析，总结档案部门在安全管理中应予关注、亟待解决的基本问题，如档案部门应该如何透过档案安全保障需求选用适当技术，现有技术策略的实施依据和目的，以

及档案安全管理策略与技术之间的关系等。

1.3实践工作的需求

档案管理具有自身的业务特点，除基础性的信息、系统与网络安全保障外，电子档案安全保障具有不同于其他电子政务业务系统的安全需求。第一，电子档案管理系统所存储的档案信息数据来源于其他业务系统，并要在规定时间、按照一定要求向档案馆移交，档案资源数据在异构系统间传递、交接，如何维持电子档案安全保障的连续性，同时满足档案管理的业务需要，是档案保管安全需要解决的重要问题。第二，电子档案管理系统中存储的数据相对集中而复杂，就档案利用而言，归档前，文件形成部门对文件具有完整的处理和利用权限；归档后，文件转化为档案，其管理权限则归档案部门所有，由档案部门管理档案利用权限，业务部门之间通过档案部门相互共享档案。这些变化相应地对利用权限的管理提出更多要求，如何确保电子档案实体安全和档案规范利用，是电子档案利用安全需要解决的重要问题。可见，以信息安全保障的一般要求来指导电子档案安全保障的实践具有一定的局限性。面向档案实践工作的需要，应当思考电子档案管理系统与其他信息管理系统在安全保障上的区别，结合档案部门的管理职责与管理流程，提炼安全保障的核心目标以及相对而言更加突出的安全需求。

（1）档案保管安全的核心要求

本文所指的“档案保管”具有较为宽泛的内涵，主要指电子文件归档后、电子档案移交前对档案进行维护性保管的过程。电子档案的真实性与长期可读性是电子档案保管阶段安全保障最核心的要求，安全保护的根本目标是防止电子档案失真、失效、丢失、缺损、不可读。电子档案的真实性有两层涵义：一是电子文件的形成过程可靠，即形成过程被认可，具体要求包括发文与收文双方的合法身份得到确认，行文正当，并在可靠的文件系统中形成与传递；二是电子档案内容、背景

和结构信息真实，具体要求包括上述三要素得到固化，并在传输、保管、迁移过程中继续保持原有的固化形式，信息完整，信息不被篡改。［13］从上述两个层面看，虽然文件阶段的真实性本刊连载不由档案部门决定，但档案真实性的维护却是档案部门的重要责任。电子档案的真实性程度来源于多项要求的叠加，满足要求项越多，其真实性程度就越高，即被认为具有更高的凭证性价值，以及更高的司法可采性。因此，我们认为，维护档案的真实性是电子档案保管过程中安全保障的一项根本目标。长期可读包括长期性与可读性两个方面：长期性意味着电子档案实体在长久的时间内不被损坏、丢失；可读性意味着电子档案信息内容在长久的时间内都可以被读取和解析。长期性与可读性应该统一为一体的保管要求，单一的长期性或可读性都无法满足档案管理与利用的需要。与传统档案管理相一致，长期可读性也与载体安全有着密切关系，物理载体的安全情况影响着电子档案的长期可读。电子档案长期可读性的其他影响因素还包括归档文件的格式和自然因素等，这些因素主要体现在档案保管工作中。电子档案管理系统肩负着将档案移交至档案馆的责任，因此，对于电子档案保管而言，保障电子档案长期可读是面向档案永久保存与未来利用的根本要求。

（2）档案利用安全的核心要求

电子档案利用过程中的安全保障，关键在于防止实体损害和越权利用，原件维护和利用控制是档案利用过程中的核心安全保障需求。在纸质档案管理中，为了防止损坏原件，在某种情况下会通过提供复制件的方式满足档案利用需要。对于电子档案管理而言，出于对电子档案实体的维护，同样可以采取副本利用的安全措施。所不同的是，基于电子档案管理系统的档案副本存储与利用面临更为复杂的情况。因为纸质档案的副本主要以复印件或缩微方式形成，副本利用对原件管理几乎不造成影响；而基于副本利用的电子档案安全保障则与电子档案原件管理模式具有密切关系。因此，电子档案原件维护是利用过程中安全保障的关键问题之一。电子档案

利用需要通过权限控制来保障信息内容安全。在电子档案管理中，档案管理者与利用者之间增加了电子档案管理系统这一中间平台，使得档案利用权限必须通过系统平台加以控制和管理，这是电子档案利用与纸质档案利用的不同。除此之外，在电子政务环境下，电子档案管理系统存储的档案资源集中而复杂，档案利用权限的管理问题更为突出，需要与传统利用审批制度相结合，从技术和管理上规范电子档案利用，这是电子档案利用与其他信息资源利用的不同。因此，电子档案的利用控制是档案利用安全保障的重要目标。我们认为，档案工作强调连贯性和流程性，安全保障的措施也具有连续性，然而某些安全保障要点在特定的管理环节中会显得尤为突出和重要。因此，我们提炼出重要的安全需求与根本的安全目标，并放置于档案保管和利用的流程背景下进行分析，旨在更好地结合档案管理实际进行探讨。

2电子档案保管阶段的安全保障

电子政务系统中的电子档案保管承接自业务系统的电子文件归档，并承担向档案馆移交的责任。这一阶段的安全保障以维护档案的真实性、长期可读性为核心目标，档案保管需采取专业性的管理措施和技术手段，防止电子档案受损、失真、不可读，保障电子档案与归档时的状态一致。

2.1建立凭证信息，维护真实性

在归档环节，为保障管理权限交接和管理责任明晰，档案部门需对接收到的电子档案进行真实性确认；在后续档案管理工作中，档案部门则需对文件归档时的真实性进行维护。［14-15］根据interpares的研究成果，档案部门保障电子档案真实性具有两层含义：一是能够证明电子档案归档时的可靠性得以维护，即档案来源身份与原始状态可证；二是能够证明电子档案保管链的完整性，即保管过程可追溯、可审计。［16-17］在理论层面，电子档案真实性的内涵实际包含了档案要素完整和档案内容可靠的要求；在实践层面，这种真实

性则表现为电子档案具有凭证性作用。针对电子档案的真实性保障与真实性认定，档案界已经开展了多方面的探索。按照实施对象与保障目标的不同，目前电子档案管理系统中主要的档案真实性保障策略可以归纳为三类：

（1）使用数字签名、时间戳技术。这是信息安全保障中普遍使用的技术手段，是针对电子档案内容和来源（即档案实体）的真实性保障措施，其目的是确保电子档案内容无损、未篡改、非伪造。其基本原理都是利用了哈希（hash）算法、数字摘要技术和非对称加密技术，通过第三方认证，用以确认电子档案状态如初、来源可信。本质上而言，时间戳是数字签名技术的另一种应用形式，可以证明某份数字文件在某一时间起就已存在。二者都满足我国《电子签名法》对于原件属性的要求，具有司法层面的可靠性。在技术上，二者都基于数字摘要对电子档案的真实性进行验证，但实现机制各有特点：基于pki（公钥基础设施）体系的数字签名技术由档案形成者采用私钥加密自行签名，验证者向第三方认证机构（由国家授权的ca认证机构）求证；［18］可信时间戳技术则由第三方机构（国家授时中心建设的时间戳服务机构）采用私钥加密签名，包含时间戳的生成日期和时间，用户自行验证。［19］然而，数字签名技术被认为具有一定的局限性，数字证书的有效期、私钥的安全性等问题使其难以满足电子档案管理的需求。［20］加入时间戳的数字签名则可以在一定程度上解决数字证书的有效性问题，使得电子档案在数字签名失效后仍具备原件属性。［21］对于电子档案真实性保障而言，它们在技术上通过加密算法来发挥作用，在机制上依赖于电子档案应用主体对第三方机构的信任，主要应用于电子档案真实性认定，属于确认性措施，并不能对电子档案受损、失真防范于未然。

（3）构建复合型电子档案身份标识。综合上述基础技术与策略，档案界提出利用非对称加密算法为电子档案构建唯一的凭证性身份标识。相较而言，构建复合型的电子档案身份标

识是一种综合的真实性安全保障策略，基本涵盖了电子档案实体与管理过程的保障需求。这一策略的基本原理是利用特定的语义算法，抽取电子档案的来源性元数据（“有效元数据集”）进行计算，生成电子档案的凭证性编码，并与相应的元数据集、来源单位及其数字签名共同构成一个电子档案凭证（“电子档案身份证”），通过凭证库管理机制实现电子档案身份的验证。［27］凭证信息可以在电子文件归档时就生成，便于在后续的保管与利用过程中进行验证，并为档案移交奠定基础。本质上，构建电子档案身份标识是综合了数字签名技术、语义算法、元数据管理等手段的复合型策略，其实现机理与数字摘要技术相似，并且因纳入凭证库管理机制而更加具有可靠性。然而，电子档案凭证信息本身的长期保存仍然是有待解决的问题。［28］综上，在电子档案管理系统中，电子档案真实性的保障措施主要针对档案实体和管理过程两个方面制定，这与档案部门对真实性保障的两个职责相对应，即确保档案来源身份与原始状态可证，以及保管过程可追溯、可审计。在保障策略方面，前者离不开基于pki体系的数字签名技术及其实现原理，后者则离不开元数据管理。电子档案管理系统从业务系统接收电子档案，来自业务部门的数字签名与原生元数据都必须受到保护和一定程度的固化，从而明确电子文件归档前后的状态与责任。在档案保管过程中，通过对数字签名、元数据与档案本体的封装与再签名，集成并关联电子档案的凭证要素，建立起连续可溯的档案保管链。从管理层面上看，现有的电子档案真实性保障策略强调档案保管过程与责任主体密切关联，并纳入第三方机构来巩固这种保管责任的可溯性与可靠性；从技术层面上看，现有策略实质上将电子档案“中心化”，即强调采用多种方法形成电子档案的附属性、凭证性信息，利用凭证信息支撑电子档案的真实性，并通过比对凭证信息来证明电子档案真实可靠。因此，在电子政务系统环境下，电子档案真实性保障的关键在于凭证信息的管理与维护。

2.2完善档案封装，确保长期可读

保障电子档案长期可读是一项连续性的工作，从电子文件归档开始便要对其采取措施。对于电子档案管理系统而言，保障电子档案长期可读的主要任务是对电子档案实体进行一定的处理，使之满足长期可读的格式和存储要求，维持电子档案的可读性，防止其丢失、失效，这是提供档案服务利用、向档案馆移交和延续至永久保存的前提□oais模型是目前电子档案长期保存普遍使用的基本策略，它所描述的功能模型、信息对象与信息包结构模型、本刊连载信息包转换过程、迁移模型都是现有长期保管策略的主要依据。具体而言，保障电子档案长期可读是要确保电子档案在长期甚至永久的保管时间内可以被读取，并可以被理解。目前电子档案管理系统中主要的档案长期可读保障策略可以归纳为以下两类：

（1）格式管理。格式管理是针对电子档案实体数据的一种基础性保障策略，通过对电子档案进行标准化、可持续的管理，防止电子档案因保管环境的变化而受损，导致无法读取、无法理解。一般认为，长期保存格式应当具有开放性、标准性和稳定性；［29］在实践层面，行业标准□da/t47-版式电子文件长期保存格式需求》更加具体地明确了长期保存格式应当满足的11点要求，包括格式开放、不绑定软硬件、文件自包含、格式自描述、显示一致性、持续可解释、稳健、可转换、利于存储、支持技术认证机制和易于利用。［30］围绕电子档案的长期保存格式，主要的保障策略包括格式注册和格式转换。格式注册主要是记录电子档案格式的描述信息和软硬件要求等，以便于对电子档案进行解析和恢复。［31］格式转换则是将电子文件或电子档案统一转换成有利于长期保存的标准格式，［32］这种转换包含两种情况：一是电子文件归档时的格式固化，如将文件固化为pdf版式文件；二是电子档案信息包的格式转换，如oais模型下提交信息包转换为归档信息包。对于电子档案管理系统而言，格式转换往往通过标准规范、统一接口或专门的格式转换平台实现。

（2）基于封装包的数字迁移。这是针对电子档案实体数据及

其运行环境的保障策略，目的是使电子档案够稳定地应对长期保管中可能面临的环境条件变化。一方面，采用开放性描述语言对电子档案及其元数据进行描述和封装可以保障电子档案信息内容在长时间内稳定、可解析□oais模型认为，要达到信息长期保存的目的，必须要存储比数字对象内容更多的其他信息要素（元数据等），［33］因此，电子档案应该以封装信息包的形式保管和提供利用□□da/t48-2009基于xml的电子文件封装规范》中规定的基于xml的veo结构封装包能够满足资源自包含、自描述、自证明的长期保存要求，［34］是目前普遍应用于电子政务环境中的档案保管策略。另一方面，数字迁移是指在必要的情况下将电子档案从某一软硬件环境向另一种软硬件环境转移的过程□oais模型中的数字迁移是基于电子档案封装包进行的，包括更新□refreshment□□复制□replication□□重新封装□repackaging□□转化□trans□formation□4种具体方式，其中后两者会改变比特序列，前两者则不会，后两者还可能涉及电子档案存储格式转换。［35］“迁移是对付技术过时的最佳良策，它应是数字资料完成定期转换的一系列有组织的工作，包括维护数字对象的真实性、用户的再检索、显示与其他利用的能力。”实践也表明，迁移是目前维护电子档案长期可读的最佳方法。［36］对于电子政务系统中的档案保管而言，电子档案长期可读性的保障措施主要针对电子档案实体和运行保存环境两个方面制定。从现有的相关保障策略看，一方面，电子档案的存储格式和存储形式必须满足开放性、不依赖软硬件环境、可解析等要求；另一方面，对电子档案存储软硬件环境和平台的管理也是必须的，这种管理主要体现在为电子档案选择稳定性高、依赖性低的保管载体和运行环境，并在必要时候开展基于档案封装包的迁移，这与纸质条件下为纸质档案构建安全保管环境的做法相同。在电子档案管理系统中，现有的电子档案长期可读性保障措施具有两个特点：一是在管理层面强调电子档案数据结构与信息描述的标准化，维持对保存环境较低的依赖性，并要求保存环境具有较高的稳定性；二是在技术层面，其基本理念是将电子档案及其元数据要素“解

构重组”，从而形成易于解析的电子档案封装包，并通过适当的转移维持档案的保存与运行条件。因此，在电子档案管理系统中，档案长期可读性保障的关键在于解决电子档案及其元数据集成封装与拆封解析的稳定性、独立性（即不依赖软硬件环境）。

2.3电子档案保管阶段的安全保障要点

对于电子政务系统中的档案保管而言，真实性与长期可读性是安全保障的双重目标，针对二者的策略也应该相互支撑，形成协同一致、自成一体的档案安全保管方案。然而，目前所采取的保障措施和提倡的保障策略难以很好地兼顾真实性和长期可读的双重要求，甚至在具体策略之间具有目前未能解决的矛盾，导致电子档案保管的安全保障工作难以高效开展。电子档案真实性与长期保存面对电子档案实体、凭证信息和档案保管过程记录三类对象。后两者相对于档案实体而言都属于冗余信息。电子档案实体本身的长期可读可以通过格式管理、规范化封装以及数字迁移得到较好解决，而凭证信息和保管过程记录则增加了长期保存策略实施的复杂性。对于上述三类对象，是否应当实施统一的对象化管理，以及如何进行管理是解决电子档案“长期真实性”保障需要考虑的问题。从目前主要的真实性和长期可读性保障策略看，较为突出的矛盾有以下两点：

（1）凭证信息的应用与长期保存之间的矛盾

无论是数字签名、时间戳还是电子档案身份标识，这些措施中所使用的技术背后都有较为复杂的实现机制，离不开第三方机构提供的信任认证。由于这些技术的应用本不是以长期保存为目标，因此并不能保证具备长期生效的能力。具体而言，电子档案真实性的根本在于信任，档案保管的长期性则要求维持这种信任。在真实性方面，现有策略中，电子档案真实性保障的关键依赖于凭证信息；在长期可读方面，最为理想的策略则要求档案信息数据不依赖于特定的软硬件，能

够做到自我解析。然而问题在于，目前凭证信息的外部验证机制难以达到长期保存对于电子档案信息数据“独立性”的要求，因而难以做到长期保存和长期有效。一方面，在目前普遍应用的基于pki体系的数字签名技术中，离不开以数字证书为基础的公钥信任，而数字证书具有时效性，数字证书过期失效意味着数字签名无法被认证。尽管增加使用时间戳可以证明数字签名在证书过期之前是有效的，弥补了数字证书时效性的局限，同时可以证明电子档案未被篡改。但数字签名和时间戳的应用是零散性的，即每一个责任主体在执行一项重要行为后，如在归档、鉴定、处置、移交等环节，可能都需要使用数字签名和时间戳。因此，在电子档案的保管过程中，为了明确责任主体和形成完整保管链，可能会形成多个数字签名与时间戳，电子档案会具有多个形成于不同主体和不同时间的凭证信息。如何对多套凭证信息进行管理是需要解决的问题。另一方面，电子档案身份标识的特点在于，标识作为凭证信息具有唯一性，可用于电子档案原始内容的反复验证，并主要通过元数据分类管理来实现保管过程的记录。［37］但电子档案身份标识的长期保存以及管理性元数据的封装问题仍然有待进一步解决。

（2）元数据更新与档案封装之间的矛盾

在电子档案管理过程中，为了确保档案保管链完整，管理性的动态元数据需要被不断添加到电子档案元数据中，而电子档案长期可读的策略主张将电子档案及其元数据进行封装。因此，如果需要对电子档案元数据进行整体封装，元数据更新会使得档案信息包面临反复封装。协调电子档案真实性与长期可读性的保障需求，需要进一步完善元数据管理与封装方案。实际上，电子档案长期可读所要求的可解析性主要是针对档案内容和自然属性元数据而言的。从微观层面上看，目前的电子档案元数据项目纷繁复杂，实践中并非所有元数据都具有长期保存的必要性。因此，一方面，对电子档案元数据进行区别分类是必要的，应该明确不同元数据对于真实性管理和长期可读的作用，据此优化电子档案的信息封装方

式与长期保存方法。另一方面，还应进一步完善电子档案的封装方式，在元数据管理的基础上，寻求满足元数据更新需求的封装方法，兼顾基于元数据的真实性管理和基于封装的长期保存要求。在电子档案管理系统中，电子档案保管阶段主要存在真实性与长期可读性保障需求难以协调的问题，导致电子档案的安全保障仍然面临许多内在的漏洞和风险。要真正实现电子档案的“长期真实性”保管，应进一步明确电子档案实体、凭证信息和保管过程元数据三类对象的保存与应用需求，兼顾电子文件归档和电子档案移交的现实需要，完善保管阶段的安全保障策略。

3电子档案利用阶段的安全保障

电子档案复制传递的高保真性、信息与载体的可分离性等特点，在给档案管理者和利用者带来方便的同时，也存在容易泄密、复制、扩散和损坏等安全隐患。因此，在电子档案提供利用的过程中，既要保护档案原件不受损坏，也要控制档案信息的利用范围，防止泄密。

3.1副本利用，保障实体安全

在纸质条件下，对于一个档案室而言，要形成一套完整的、同质载体的纸质档案副本，几乎是不可能实现的。因为这样做意味着要建立一个与已有室藏规模相当的库房，并且需要投入大量时间进行复制，时间、管理与经费的投入几乎都是翻倍的。但对于电子档案管理系统而言，形成一套完整的电子档案副本则相对容易许多。《电子公文归档管理暂行办法》等法规标准中都要求，区别于封存保管的电子档案，应拷贝形成一套电子档案专门提供查阅利用。考虑到业务部门对电子档案的经常性利用多以查阅信息解决问题为主要目的，相对而言对其凭证性要求并不突出，为了避免电子档案原件在利用过程中遭到损坏或篡改，可以抽取电子档案内容信息形成电子档案副本以供查询和利用。电子档案副本的内容与电子档案完全一致，可以满足业务部门一般的信息利用需求。

［38］在生成电子档案副本以供利用时，可以根据实际情况采用不同方式。第一种是在归档时，系统自动抽取电子档案内容信息形成一份电子档案副本并加以保管，在查询与利用时直接调取电子档案副本。采用这种方式，电子档案管理系统中可以建立单独的利用数据库，用以存放所有电子档案副本，电子档案原件及其元数据则打包封存于保存数据库中，两个数据库分开管理。在进行档案编研、提供利用等活动时只需调取利用数据库中的档案副本，有利于维护档案实体安全。电子档案被移交到档案馆之后，电子档案副本仍然可以保留在电子档案管理系统中，以备提供日常利用。第二种是在利用者发出档案利用请求时，系统根据请求自动抽取相应的电子档案生成副本后提供利用，利用结束之后，电子档案副本被自动清除，这种方式被称为根据利用需求“动态打包”。这种方式可以大大节省系统的存储空间，节省存储成本，但对系统性能要求较高。综合而言，第一种方式要求电子档案管理系统具有较大的存储空间，但对于当下还未真正与数字档案馆实现互联互通的电子档案管理系统而言，可以相对完整地保留本单位形成的档案信息资源，为前端业务部门的档案利用提供便利。在真正实现了数字档案室与数字档案馆互联互通的情况下，电子档案移交到数字档案馆后，前端业务部门利用电子档案时可以直接从数字档案馆获取，此时数字档案室也无需再保留已移交的电子档案副本了，这将极大地节省数字档案室的系统存储空间与成本，大大提高资源的利用效率。

3.2三权分立，保障信息安全

针对电子档案的利用，要求电子档案能够在档案管理系统中安全运行和流转，保证合法用户的合理使用以及禁止非法用户的访问，使电子档案信息免遭破坏、更改或非法拷贝等。［39］要实现利用过程的安全保障，就要确保访问合法、利用合理、全程记录。具体而言，要做到以下三点：一是划分访问与利用权限，通过访问控制技术避免权限扩散；［40］二是控制利用行为，通过文件保护技术、版权保护技术等控

制用户对电子档案内容的非法篡改、传播、伪造、侵权等不合理利用行为；［41］三是对电子档案利用全过程实行跟踪记录，利用审计跟踪技术进行全程监控，提供事后对非法行为的追溯回查。［42］这三点要求实质上对应了利用系统中的三个角色———系统管理员、安全管理员和安全审计员。依据国家保密标准bmb20-涉及国家秘密的信息系统分级保护管理规范》的有关规定，电子档案利用系统应该配备系统管理员、安全管理员和安全审计员三类安全保密管理人员，分别负责系统运行、安全管理和安全审计工作。三类人员之间相互独立、相互制约，实现三权分立，以保障电子档案利用系统的安全。［43］（1）系统管理员系统管理员负责对访问利用的角色和用户进行设置。具体而言，系统管理员根据本单位情况，设置相应的用户角色，指定其功能权限，即为不同的利用者创建不同的利用账号。利用者根据所分配的账号登录电子档案利用系统进行查询与利用。（2）安全管理员安全管理员负责对角色和用户进行授权，将角色权限与数据对象关联起来，并进行数据的备份。具体而言，即根据用户角色的权限，配置其所能操作的相应数据对象。当利用者发起查询与利用操作时，系统自动根据利用者的身份及其所匹配的权限级别返回结果，不在利用者的权限范围内的信息内容则不予显示。同时，可以利用数字水印、网页控件技术等，对电子档案的浏览权限、打印权限、下载权限等分别进行严格的控制，［44］做到定点———只能在某台机器上打开，定人———只能由某个用户使用自己的口令打开，定时———只能在固定的时间段内打开，定次———只能打开固定的次数。同时，还可以实行防复制、防下载、防打印等。［45］（3）安全审计员安全审计员负责全程审计跟踪电子档案利用过程。具体而言，一是对系统管理员和安全管理员的行为进行审计跟踪，确认系统管理员和安全管理员的操作行为合法、合规；二是对安全管理活动的相关信息进行识别、记录、存储和分析，记录、存储用户的利用行为，并对恶意攻击行为进行识别和处理，及时发现和阻止各种来自外部的非法入侵行为以及内部用户的非授权活动。档案利用系统中三类管理员与利用流程的对应关系如图1所示。

3.3全程记录，维护元数据完整

iso23081-2中指出，档案管理元数据必须具备:（1）档案本身的元数据；（2）业务规则或政策及授权元数据；（3）责任者元数据；（4）业务活动或过程元数据；（5）档案管理过程元数据；（6）有关元数据的元数据。［46］凡是用来描述电子档案管理的元数据，没有全部覆盖以上范围者，对于电子档案管理的描述是欠缺完整的。［47］在副本利用方式下，电子档案副本的形成、利用和管理是档案利用过程元数据积累的主要来源，尽管这些元数据围绕电子档案副本而形成，但却是电子档案利用过程的重要记录，应该与电子档案原件关联，作为电子档案利用情况的全程记录。具体而言，一方面，在生成电子档案副本的过程中，涉及责任主体和复制过程的相关信息十分重要，需要被保存下来，具体包括：档案复制的日期及责任人，从生成者那里获得的档案与由保管者产生的拷贝之间的关系，复制过程对其形式内容、可存取性及使用的影响等。另一方面，在副本的利用与管理过程中，所积累的元数据和档案管理过程的元数据一起，共同组成电子档案管理系统（档案室）阶段的管理过程元数据。也就是说，业务部门在利用档案副本时会积累各种利用信息，档案部门在管理档案副本时也会积累各种保管信息，针对档案副本形成的这些记录需要被妥善保管，作为电子档案利用与副本管理的元数据。这部分元数据主要包括利用权限、密级划分、利用对象、利用时间、利用频率等信息，它们以动态元数据的形式积累，反映了电子档案的利用情况，可以为后续电子档案的管理与利用提供依据。除此之外，电子档案副本管理中产生的利用日志元数据，与电子档案管理过程中产生的管理日志元数据一样，［48］都是电子档案“从其生成时就已遭受的各种变化的信息”，［49］应该得到妥善保管。在电子档案移交给档案馆时，副本管理的利用日志元数据可以与电子档案封装包关联，提供给档案馆以作参考，辅助管理。

3.4电子档案利用阶段的安全保障要点

在电子档案利用的过程中，应该保护档案的完整性和真实性，并确保涉密档案信息不受侵害。［50］具体到电子档案的管理中，其核心要点可以概括为以下两个方面：（1）保护电子档案实体与信息安全电子档案管理系统作为档案流动的“中部枢纽”，确保所接收的档案完整、真实、可用是基本的业务要求，有此基础，才能为前端业务部门提供真实有效的档案信息资源，并为后端档案馆输送真实、完整的档案。因此，在提供利用的过程中，仍然应该把确保电子档案的真实性、完整性、安全性作为第一要务。这就包含两个方面的内容：一是保证电子档案实体安全，使其不被破坏、不被丢失；二是保证电子档案信息安全，使其不被越权利用、不被违规扩散。同时，通过全程审计跟踪记录用户的利用行为、系统管理员的操作行为，作为工作查证的依据，以供事后审核。目前在具体的操作中，提供电子档案副本利用，可以确保电子档案的实体安全。在档案信息安全方面，则可以通过利用系统三权分立监管档案利用行为，从授权登录、利用过程到全程审计对用户的利用行为进行监控；结合使用身份认证、审计跟踪、文件保护、数字水印等技术，可以防止档案信息的越权利用；还需根据利用者的利用请求与权限情况，只将权限范围内允许的档案信息打包传输到终端予以显示，并严格监控其利用行为。（2）保存完整的元数据加拿大律师肯萨斯认为：“电子档案成为证据必须具备三个条件：一是记录或存储电子档案的系统的完整性，二是电子档案的真实性，三是电子档案是在通常的、正常的业务过程中产生、处理和保存的。”［51］简单地说，就是要注重系统、电子档案、形成过程这三个要素。［52］在电子档案提供利用的过程中，保存利用过程中的元数据，记录电子档案信息资源的利用者、利用时间、利用频率等具体的利用过程信息，一方面可以对电子档案信息安全进行跟踪记录，以备查考；另一方面也能够为移交进馆之后的电子档案管理活动提供参考依据。在电子档案提供利用的过程中，同样可以参考纸质档案利用的安全保障对策：一是副本利用，纸质档案利用在不要求凭证性的情况下会提供复制件以满足一般的信息利用需求；在电子档案利用中，则可以抽取电子档案的内容信息形成电子档案

副本以供查询和利用，维护电子档案原件实体。二是完整的元数据记录，纸质档案利用中使用档案利用登记表用以记录档案的利用情况；在电子档案利用中，则需要对电子档案副本的利用过程进行全程审计跟踪，并保存利用过程的元数据。除此之外，与纸质档案管理所不同的一点在于，在电子档案管理系统中，需要以安全管理的三权分立为基础来实现电子档案的利用控制，设置系统管理员、安全管理员和安全审计员三类角色，对其安全管理权限进行互相制约，以保证从用户授权登录、查询利用和全程监督审查的整个利用过程都处于可控范围内，防止对档案信息资源的越权获取、越权使用。

4电子档案管理全流程的支撑性安全保障

电子档案管理系统离不开面向档案管理全流程的支撑性安全保障措施，用以巩固电子档案管理系统的安全管理。贯穿于档案管理全流程的支撑性安全保障措施主要包括四性检验和档案备份，二者与保管和利用中的阶段性保障策略相辅相成，在电子档案管理系统中共同保障电子档案安全可控。

4.1四性检验，实现档案质量跟踪

确保电子档案真实、完整、可用、安全是电子档案管理的核心要求。《电子文件管理暂行办法》和《电子档案移交与接收办法》分别要求，在电子文件归档和电子档案移交时，应对电子文件和电子档案的真实性（也称“准确性”）、完整性、可用性、安全性进行检测，这四点要求统称为电子档案“四性”。就其实质内容而言，实践中的四性检验等同于档案管理理论上的技术鉴定，贯穿于档案管理全流程。四性检验的意义主要体现在两个方面：一是控制档案质量，在归档、移交等工作中，以及在需要对电子档案进行迁移、格式转换或传输的情况下，都意味着存储状态、存储系统和管理环境将发生变化，对档案进行四性检验可以使档案接收方或新的保管环境掌握档案质量情况，对于不符合质量要求的档案，可以及时采取措施保障档案安全可控，避免档案质量的

进一步损害；二是明晰交接责任，归档和移交都意味着档案管理责任主体将发生变化，规范化的四性检验可以避免缺损档案处理中的主体模糊，有利于明确处置职责，及时维护档案安全。对于电子政务系统中的档案管理而言，贯穿管理全程的四性检验实质上是以动态的形式保障电子档案安全。具体来说，真实性检验要求档案目录信息、内容信息及相关数据信息准确，及数据包规范；完整性检验要求数量和数据两个方面的完整；可用性检验要求数据、内容可读，以及软硬件环境满足长期保存需求；安全性检验则要求档案安全标识规范，并要进行病毒检测、漏洞筛查等。四性检验在电子档案整个生命周期中具有不同的应用需求，在不同情况下，四性检验的侧重点也有所区别。在具体操作中，可以根据管理主体和保管环境是否变化，通过检验功能组配，选择必要的检验项目，达到情境化、高效率的检验效果。在电子档案管理系统中，主要的四性检验节点有三个，分别是文件归档、档案保管与档案移交。在文件归档和档案移交阶段，因管理主体和保管环境都将发生变化，要对电子档案进行全面的四性检验。在档案保管过程中，一方面，应着重开展周期性的真实性、可用性检验，防止档案被更改、不可读；另一方面，在档案利用、档案迁移等情况下，则应该着重开展完整性、安全性检验，防止档案缺损或感染病毒。四性检验具有零散性的特点，在档案管理全流程中，应该根据具体环节中档案内容、档案载体、系统环境、管理主体变化情况，选择具有针对性的检验内容，并及时执行检验。四性检验也具有系统性的特点，在档案管理全流程中，不同环节的四性检验具有不同的侧重点，与不同阶段的档案管理工作需求相契合，可以对电子档案全生命周期的质量控制进行全程保障。

4.2档案备份，提供档案全程保障

数据备份是信息安全保障重要的支撑性措施，在检验性、确认性安全措施的基础上，数据备份可及时、有效地弥补数据缺损、数据失真和数据丢失等漏洞，甚至在面临自然灾害、系统故障等情况时，也可以通过备份数据的恢复重建信息资

源。在传统档案管理中，异质、异地备份是档案安全保障的重要措施，对电子政务系统中的档案管理而言同样如此。所不同的是，电子档案备份不再仅以支持灾难预案为目的，而更加突出档案保管、档案利用等环节的安全需求，以为电子档案管理全流程“护航”为目的。电子档案备份应伴随电子档案全生命周期而存在，与数字迁移、副本利用、四性检验等措施相结合，构建更为稳固的电子档案安全保障。电子档案备份工作越来越受到重视。在战略规划方面，《-国家信息化发展战略》关于建设国家信息安全保障体系的要求中明确应重视备份建设；全国档案工作会议以及20、全国局馆长会议都强调档案安全备份的重要性，提出对电子档案实行异质、异地备份。在法规标准方面，《电子文件管理暂行办法》、《电子公文归档管理暂行办法》、《电子文件归档与管理规范□□gb/t18894-□□□cad电子文件光盘存储、归档与档案管理要求□□gb/t17678.1-□□都明确电子档案管理应建立备份，要求电子档案实行三套保管，一套封存保管，一套提供利用，一套异地保存。目前，以电子档案安全保管为目的的备份主要采取异质、异地备份相结合的策略；以电子档案安全利用为目的，则主要采取异质备份策略。电子档案异地备份的实施策略与传统条件下大体相同。对于电子档案异质备份而言，从备份介质上看，包括磁盘阵列、磁带机、光盘、硬盘等多种设备，应当结合实际情况加以选择。然而，最为理想的做法是，对于适宜长期保存的载体，应对电子档案进行同质、异地备份，这将更有利于电子档案保真。电子档案管理系统中的档案备份与档案馆备份措施之间的关系需要进一步明确。

在传统纸质档案管理中，档案备份并不是机关档案室的主要工作内容，备份工作主要由档案馆承担。在电子档案管理中，由于电子档案具有数字化信息的不稳定性特点，出于基本的信息安全考量，在电子档案管理系统中也需要对电子档案进行备份。与传统纸质档案管理相比，电子档案的备份工作应该提前到归档后的档案保管阶段，并且备份应随电子档案一同移交至档案馆。在档案室与档案馆之间，电子档案的备份工作应该具有连续性。首先，电子档案管理系统需要进行档

案备份，这是计算机网络与信息系统管理条件下的基本要求，同时国家《数字档案室建设指南》中也作了明确建议，因此电子档案管理系统进行电子档案备份是电子档案管理的基础性需要。其次，在实际工作中，一些电子档案管理系统在向档案馆进行电子档案移交时，往往是异质多载体、多套移交，在本质上已经实现了电子档案及其备份的同时移交。再次，通过调研得知，对于档案馆而言，馆藏电子档案的数量往往是数百t级别甚至更大，完全由档案馆承担从无至有的电子档案备份，其工作量是巨大的，进行一次省级综合档案馆馆藏的完全备份有时需要一个月甚至更久。因此，基于高效率、集约化以及安全保障管理的综合考量，我们认为，应当在电子文件归档后，对电子档案进行备份，并在电子档案管理系统内，实行科学的备份机制；在向档案馆移交电子档案时，一并移交经过周期性维护的备份档案，以及备份管理的日志记录等。这不仅有利于电子档案管理系统开展规范化的备份管理，在电子档案交接后，也有利于档案馆对备份档案开展连续性管理，避免不必要的重复备份，在一定程度上有助于提高档案馆的工作效率。电子档案的四性检验与档案备份对于电子档案管理全流程的安全保障具有支撑性作用。保管与利用阶段的安全保障措施侧重对电子档案进行阶段性的直接保护和监管，而支撑性的安全保障措施则贯穿于电子档案管理全程，提供面向全流程的保障。四性检验作为综合性的检测措施，可以实现档案质量的跟踪，并为管理结点与交接环节提供基础而必要的安全保障；档案备份则可以切实起到电子档案的安全保障作用，尤其在发现档案数据缺损或丢失时，完善的备份恢复机制是目前保障档案实体安全的最佳对策。

5结语

研究档案信息安全保障问题，是解决电子档案“保得住”的关键，是开展档案资源整合与利用、联通与共享、移交与长期保存等后续工作的重要前提。电子档案管理的安全保障应该在信息安全的基础上，结合档案管理的流程特点与业务需求，提炼安全保障的关键要点，寻求更加契合档案管理实际

的安全保障对策。本文以电子政务系统中的档案保管与利用为框架，分别对这两个阶段以及电子档案管理全流程的支撑性安全保障策略与要点进行了梳理和分析。电子档案的安全保障应当具有连贯性，并与管理流程紧密结合。综合而言，电子档案保管阶段应关注凭证信息的长期保存以及档案封装方式，协调真实性与长期可读性的保障要求；电子档案利用阶段应关注电子档案的副本利用及其元数据的管理；对于电子档案管理全流程而言，则应关注四性检验的实施方案，以及电子档案管理系统进行电子档案备份及其移交的模式与方法。虽然不同的电子档案管理系统需要根据实际情况采取不同的安全保障策略，但基于共性的档案管理流程，梳理共性的安全保障需求与要点，可以充实档案安全保障的实际内容，从而更好地有的放矢，根据实际需求选用适宜的技术和管理方法，完善电子档案系统中的档案管理安全保障。

光谷一路电力改造篇三

在当前我国电力系统系统发展中，依旧有一些制约因素存在，并且主要表现在两个大的方面，一方面是在外送过程中电网存在的问题；另一个方面是供电网的供电末端有一定问题存在。该问题的存在主要是由于我国在初期建造电力系统的过程中，没有给予用户对电网使用建设高度重视。为了能够与当代技术发展相适应，充分的满足用户对电网使用各个方面的要求，改革已经成为了重要举措。

1对电力系统的运行现状分析

由于我国在电力系统发展方面依旧较为落后，因此，当前在电力系统运行中还有很多问题存在，这些问题主要表现在以下几个方面，即：

1.1电力系统的荷载没有均衡分布

目前，由于我国在电网设计中还使用较为传统的设计方式，

为此在设计中还有一些不合理的现象存在。加之我国各地区发展不够平衡，导致电网和在区域以及无荷载的区域内划分不够平衡，这导致出现了电路负荷载功率同样出现了不平衡的问题。例如：有一部分地区还处于发展的阶段，当前供电网所有供电能力已经无法满足居民电力供应需求，这导致供电网出现了超负荷运行的问题，在这种情况之下如果电网继续运行，必将损耗极大的功率，这会导致出现能源浪费的现象。为此，应该彻底的改造国家电网系统，从而有效避免在用电过程中给电器设备带来损害。

1.2配电设备缺少合理布局

当前在电力系统布局中依旧有布局不合理问题存在，当前在不同地区的发展中依旧存在着极大的差异，如果在供电体系设备布局方面依旧采用传统的布局方式进行布局，那么势必会给电力消费的分配带来不合理的结果，同时也会给用户的正常用电以及生活带来消极的影响。为此，在电力供应的整个过程中，应该对各个地区的经济发展水平进行严格的调查，从而合理的分配电力供应。部分供电单位为了能够减少在电网改造方面的资金投入，没有适当的更新原有的线路以及设备，而是直接的把一些新的设备引入到原有的电网设备之中，这种行为给电网带来了极大程度的影响，同时也会导致出现一系列的不良反应，给电网系统的正常操作带来冲击。

1.3配电设备陈旧

在近年来检修电网过程中已经发现，有很多地方的电网线路已经出现了老化的问题，并且供电设备陈旧，如架空线比较陈旧，电缆线使用的时间过长，也有部分电缆线出现了老化的问题。同时，隔离开关、配电变压器以及一些其他的设备陈旧落后，无法与现代供电设备要求相符合。如果不及时的更新设备与线路，必将会给电力系统的自动化管理带来消极的影响，同时也会出现资源浪费的现象，这会严重的冲击电力行业的发展。

2改造电力系统应该坚持的原则分析

由于我国的基本国情和各个方面因素的存在，如果要对电力系统进行重新的建设与规划，必将会成为一项艰难的任务，为此，最为适宜的方式就是在原有的电力系统基础上适当的进行改造，从而能够与当地电力系统基础要求相符合，从而为改造电力系统技术提供保障。为了能够保证改造后的电力系统符合用户的用电要求，相应的电力部门必须要编制好统一的规划设计，放远眼光，从而确保改造电力系统过程中所使用的设备以及改造技术等能够与现阶段的发展要求相符合。为此。在改造电力系统的过程中，应该坚持以下几个方面的原则，即：

（1）确保供电线路以及供电设备的质量；

（2）应该保证改造技术的先进性，使之与当地的地区经济发展趋势相符合；

（3）要确保改造以后的电力系统运行和维护工作简单，确保电力系统能够高质量的运行；

（4）要确保电力系统在改造以后，能够有充足的安全性与经济性作为保障。

光谷一路电力改造篇四

（1）职工自身安全意识差。

目前的电力系统管理部门并没有很好的处理安全与稳定、发展和企业业绩之间的关系，在生产过程中安全责任意识淡薄，职工们并没有真正意识企业安全生产的重要性。部门员工总是习惯性的违反企业的安全规章制度。管理人员在检修设备过程中由于安全意识差总是存在违反安全组织措施和相关的技术措施，造成不必要的人员伤亡和电网设备的无故损坏。

（2）电厂企业领导安全管理意识差。

在某些电力企业中领导并没有处理好安全和生产的关系，总是重生产而轻安全，在处理安全生产问题时总是不能做到居安思危，安全管理的常规工作做得不是特别认真和到位，只有出了安全问题后才开始进行处理。其中的原因可能是多方面的，但是其中“人情”因素是最为重要的一个因素。

（3）管理人员责任心不强。

新入职的职工在对安全管理制度没有完全理解就投入了工作当中，出现相关问题时为了省事就直接按照自己个人的理解对事情进行处理并没有完全按照企业的相关规定进行处理；工作多年的管理人员在出现问题是则会习惯性的根据自己多年的经验进行处理，也是没有按照规范的操作流程进行处理。这些安全责任心不强的表现都会对安全生产带来非常大的危害，这些行为无形中已经留下了非常多的安全隐患。

光谷一路电力改造篇五

供电企业作为资金技术密集型企业，固定资产管理是企业管理的一个重要组成部分。在固定资产的使用中，技术改造支出、大修费用是两项重要的后续支出。随着供电企业的不断发展壮大，技改大修工程项目越来越多，做好技改大修项目管理具有十分重要的意义。本文分析了技改大修项目的管理现状，提出一系列的管理强化措施，以此共同探讨。

1 引言

2电力系统技改大修重要性分析

技改大修体系落后

成本控制不足

供电企业在技改大修项目实施时，未能全面评价企业内部的资产，无法为技改大修提供稳定的成本，进而引发成本不足或失控的问题，造成技改大修过程中成本资金的浪费。技改大修项目管理中，需要在成本投入方面实行基本的控制和规划，优化技改大修项目的编制，防止技改大修项目出现成本超支的情况。

项目实施存在的问题