

附 页

尊敬的审查员老师，您好！

非常感谢您对本申请认真细致的审查。申请人在收到第一次审查意见通知书后，进行了认真的研究，并按照审查意见进行了修改（参见所附修改页）。具体如下：

1 关于修改

将权利要求 4 的内容合并至权利要求 1 中，并删除原权利要求 4。

由于仅涉及合并权利要求，并未超过原始权利要求书记载的范围，因此修改符合专利法第 33 条的规定。

2 关于权利要求 1 具备创造性

2.1 关于最接近的现有技术

审查员老师经过全面细致的检索，获得最接近的现有技术（作为对比文件 1）名称为“基于江西 500kV 电网的信息通信网络安全防护体系研究与设计”，要解决的技术问题为“建立信息通信网络安全防护体系”，发明构思为“根据电力信息通信网络数据分层分级原理和依据,找出通信网络现状、存在问题、以及基础设施与安全防护体系中存在的安全风险;并基于信息通信网络的基础设施安全、网络传输安全、防护措施改造、业务承载优化以及网络安全管理等五个方面提出信息通信网络安全防护体系总体方案”。

而本申请的技术主题为“一种基于流水线自动运转的安全检测平台及方法”，要解决的技术问题为“如何基于风险分析评判以及检测安全性”，发明构思为“由威胁和脆弱性确定安全事件发生可能性值，以及由资产和脆弱性确定安全事件的损失值，从而确定风险值”。

由此可见，对比文件 1 与本发明的主题以及采用的技术手段并不相同。

2.2 区别技术特征

为了更加清楚地突出本发明与对比文件之间的区别技术特征以及区别技术

特征能够带来的有益效果，本申请人经过全面对比，制作了特征对比表，如下表所示。

本申请	对比文件 1	对比文件 2	说明
一种基于流水线自动运转的配电终端安全检测系统	基于江西 500kV 电网的信息通信网络安全防护体系研究与设计	一种配电终端自动检定流水线作业方法	本申请与对比文件 1 以及对比文件 2 所要解决的技术问题均不相同
配电终端检测流水线，用于配电终端的接入和运出		自动化检测工作，将被检定的配电终端放置在第一输送线上，通过第二输送线将被检定的配电终端传送至第一指定位置，退出	
配电终端安全检测平台用于对所述安全检测系统自身以及配电终端进行安全检测	安全防护系统用于对信息通信网络及安全防护系统本身进行安全检测		
综合管控系统			
综合管控系统连接配电终端检测流水线与配电终端安全检测平台			
配电终端安全检测平台包括高性	认证/加密，安全漏洞评估，入侵		

本申请	对比文件 1	对比文件 2	说明
能配电加密认证装置、安全风险评 估设备、入侵检测 服务器、安全设备 检测装置及漏洞 扫描服务器	检测设备，安全 监测装置，扫描 漏洞		
安全风险评估设 备采用矩阵法或 相乘法计算威胁 出现的频率			
安全风险评估设 备评估脆弱性的 严重程度以及信 息资产的重要程 度			
安全风险评估设 备确定由于威胁 或利用脆弱性导 致安全事件发生 的可能性			
安全风险评估设 备综合安全事件 所作用的资产价 值及脆弱性的严 重程度判断安全 事件造成的损失			

申请人经过全面地对比，认为本申请的权利要求 1 与对比文件 1 相比，至少存在以下区别技术特征：

“连通两者进行信息交互的综合管控系统；

配电终端安全检测平台包括安全风险评估设备；

所述安全风险评估设备采用矩阵法或相乘法计算威胁出现的频率、评估脆弱性的严重程度以及信息资产的重要程度，确定由于威胁或利用脆弱性导致安全事件发生的可能性、综合安全事件所作用的资产价值及脆弱性的严重程度判断安全事件造成的损失。”

2.3 基于区别技术特征，本发明实际解决的技术问题

基于该区别技术特征，本发明实际解决的技术问题是，将安全事件的可能性结合安全事件造成的损失，分析风险值。

2.4 技术启示

从上表可知，对比文件 1 只公开了安全防护系统，其目的不是对各种安全风险进行概率上的估计。而是通过对安全风险存在的问题进行分析，从而解决安全隐患。对比文件 1 没有意识到在解决安全隐患前，可以事先进行安全风险的评估，从而更合理更高效的解决问题；同时也没有给出具体的措施以进行风险评估。因此，对比文件 1 并不存在改进为风险评估分析的技术问题，所属领域技术人员没有动机在对比文件 1 的基础上进行改进获得本发明的技术方案。

更具体的，对比文件 1 是一篇综述文件，只介绍了关于安全防护体系的大致构想，并未公开安全防护具体的技术方案。而本申请相对于对比文件 1，具体公开了如何根据矩阵法或相乘法计算威胁出现的概率、以及评估脆弱性的严重程度等具体技术方案。因此，与对比文件 1 相比，本申请着重介绍了安全事件发生的概率对于最终安全检测的影响。

需要说明的是，对比文件 1 公开了“根据不同安全区域的安全防护要求，在不同安全区域内的信息系统安全等级与防护水平不同”。并具体“将各个系统划分为不同的等级进行区别性的防护”。从对比文件 1 中的表 2.1 也可以看出，各个系统的安全等级是预先设置好的。由此可见，对比文件 1 要解决的技术问题是根据预设的安全等级，进行区别性的防护。这与本申请要解决的技术问题根据系

统受到攻击的可能性，建立不同的安全防护要求完全不一样。实际上本申请的发明要点恰恰构成对比文件 1 的先决条件。因此，二者取得的技术效果自然也不可能相同。此外，本申请明确公开了上述系统受到攻击的可能性也不是预设值，而是根据威胁出现频率及脆弱性的状况计算出来的。因此，代理人认为，本申请新的权利要求 1 将安全事件的可能性结合安全事件造成的损失，分析风险值。是具备突出的实质性特点与显著的进步，符合专利法第 22 条第 3 款的规定。

此外，对比文件 1 在安全风险分析中还公开了网络传输、安全防护措施、网络业务承载以及网络安全管理所涉及的安全风险的各个方面。但是对比文件 1 仅仅对各种情况进行了定性的介绍，并没有公开计算各个系统的安全风险的概率值，同时，也没有将安全风险分析与安全检测相结合进行分析。而本申请将安全风险分析（即由威胁和脆弱性确定安全事件发生可能性值）与安全检测（即由资产和脆弱性确定安全事件的损失值）相结合，提出了一种针对性的安全检测技术方案。具体的，本申请在安全风险分析中还公开了“应综合攻击者技术能力（专业技术程度、攻击设备等）、脆弱性被利用的难易程度（可访问时间、设计和操作知识公开程度等）、资产吸引力等因素来判断安全事件发生的可能性”。与之相对应的具体的技术手段是通过“利用入侵检测服务器，采用被动检测的方式对配电终端进行网络攻击，包括从配电终端信息采集系统网络中采集数据包。”而对比文件 1 中的入侵检测服务器的功能仅仅是用于进行入侵检测，并没有提及或公开网络攻击这一特征。在此基础上，代理人认为原权利要求 5 的进一步的限定特征本身也具有创造性。

对比文件 2 的主题为一种配电终端自动检定流水线作业方法，其要解决的技术问题为“通过流水线实现配电终端的自动化”。完全没有提及安全防护等相关信息。因此，对比文件 2 的主题与本申请的主题不一致，其要解决的技术问题与本申请不一致。同时，对比文件 2 也没有对上述区别技术特征进行公开。

因此，申请人认为，对所属技术领域的技术人员来说，本发明相对于现有技术是非显而易见的，相关技术人员没有动机在对比文件 1 的基础上结合对比文件 2，解决本发明所要解决的技术问题，本发明具有突出的实质性特点；同时，本发明克服了现有技术中存在的缺点和不足，与现有技术相比能够产生有益的技术

效果，具有显著的进步；因此本发明具备创造性，符合专利法第 22 条第 3 款的规定。

3 其他权利要求

权利要求 2-7 引用了在先的权利要求 1，由于权利要求 1 具备创造性，因此引用了在先的权利要求 1 的权利要求 2-7 也具备创造性，符合专利法第 22 条第 3 款的规定。

申请人按照审查意见对申请文件进行了修改，克服了通知书所指出的缺陷，修改文本符合专利授权条件。如果审查员认为该申请还存在其它问题，恳请给予再次修改和陈述的机会。联系电话是 010-62535882，申请人愿意配合审查员老师的意见主动修改申请文本，早日结案，缩短审查周期。

最后，再次感谢审查员老师为本案所作的认真细致的工作。