国 家 知 识 产 权 局

610000

成都市天府新区华阳华府大道 1 段 1 号蓝润 ISC2 栋 1 单元 2008 号 成都天汇致远知识产权代理事务所(普通合伙)

韩晓银(028-87763797)

发文日：

2023 年 02 月 24 日

申请号：202010471767.8　　**发文序号：** 2023022400091170

申请人：成都金隼智安科技有限公司

发明创造名称：基于机器学习的工控环境智能安全检测系统与方法

驳　　回　　决　　定

1.根据专利法第 38 条及其实施细则第 53 条的规定，决定驳回上述专利申请，驳回的依据是：

☐申请不符合专利法第 2 条第 2 款的规定。
☐申请属于专利法第 5 条或者第 25 条规定的不授予专利权的范围。
☐申请不符合专利法第 9 条第 1 款的规定。
☐申请不符合专利法第 19 条第 1 款的规定。
☒申请不符合专利法第 22 条的规定。
☐申请不符合专利法第 26 条第 3 款或者第 4 款的规定。
☐申请不符合专利法第 26 条第 5 款或者实施细则第 26 条的规定。
☐申请不符合专利法第 31 条第 1 款的规定。
☐申请的修改不符合专利法第 33 条的规定。
☐申请不符合专利法实施细则第 20 条第 2 款的规定。
☐分案申请不符合专利法实施细则第 43 条第 1 款的规定。
☐_____

详细的驳回理由见驳回决定正文部分(共 4 页)。

2.本驳回决定是针对下列申请文件作出的:

☐原始申请文件。☐分案申请递交日提交的文件。☒下列申请文件：

申请日提交的摘要附图、说明书摘要、说明书第 1-45 段、说明书附图； 2022 年 12 月 13 日提交的权利要求第 1-6 项。

3. 根据专利法第 41 条及实施细则第 60 条的规定，申请人对本驳回决定不服的，可以在收到本决定之日起 3 个月内向专利局复审和无效审理部请求复审。根据专利法实施细则第 96 条的规定，复审费应在上述期限内缴纳，期满未缴纳或者未缴足的，视为未提出请求。

国家知识产权局 专利审查业务章 1101081359734

审 查 员：冉涛
联系电话：02862969688

审查部门：专利审查协作四川中心

纸件申请，回函请寄：100088 北京市海淀区蓟门桥西土城路 6 号　国家知识产权局专利局受理处收

电子申请，应当通过电子专利申请系统以电子文件形式提交相关文件。除另有规定外，以纸件等其他形式提交的文件视为未提交。

驳 回 决 定

申请号：2020104717678

本决定涉及的是申请号为 2020104717678 的名称为“基于机器学习的工控环境智能安全检测系统与方法”的发明专利申请（下称“本申请”），申请人为成都金隼智安科技有限公司，申请日为 2020 年 05 月 29 日。

一、案由

本申请原申请文件权利要求书包括 2 项独立权利要求 1、9 以及 8 项从属权利要求 2-8、10。

应申请人于 2020 年 05 月 29 日提出的实质审查请求，审查员对本申请进行了实质审查，并于 2022 年 08 月 08 日发出了第一次审查意见通知书，指出权利要求 1-10 不具备专利法第 22 条第 3 款规定的创造性。通知书中引用了如下对比文件：

对比文件 1：CN 107612733A，公开日为 2018 年 01 月 19 日；

对比文件 2：CN 106506486A，公开日为 2017 年 03 月 15 日。

申请人于 2022 年 12 月 13 日针对第一次审查意见通知书提交了意见陈述书，其将原权利要求 4、5 的内容添加到原权利要求 1 中，并删除了原权利要求 9、10，上述修改属于技术特征的简单叠加。其意见陈述概述如下：

对比文件 1 与本权 1 中的“所述预处理模块基于本体将数据聚合，即，将工业控制系统中具有相同概念和语义的数据进行归类和抽取，将聚合得到新的数据分类，所有分类构成的集合作为机器学习的训练数据集”不同，本权 1 公开了机器学习所需训练数据集的具体数据来源的预处理过程。

审查员认为，本案事实已经清楚，因此针对申请日提交的摘要附图、说明书摘要、说明书第 1-45 段、说明书附图； 2022 年 12 月 13 日提交的权利要求第 1-6 项作出本驳回决定。

二、驳回理由

(一)、关于权利要求的创造性

1.权利要求 1 不具备专利法第 22 条第 3 款规定的创造性。

权利要求 1 请求保护一种基于机器学习的工控环境智能安全检测系统，对比文件 1（CN107612733A）公开了一种基于工控系统的网络审计和监测系统，其采用了机器学习生成白名单安全策略规则（相当于一种基于机器学习的工控环境智能安全检测系统），并具体公开了以下技术特征（参见说明书第[0034]-[0057]段）：步骤 A：流量采集模块对常见的网络应用层协议数据包做流量采集、解析还原（相当于数据采集模块，用于采集工业控制内部网应用层协议的数据包），步骤 B：进行机器学习，即在机器学习周期(即指系统部署成功后，通过配置系统的机器学习周期，计算系统运行起始时间到系统当前时间的时间差，当系统运行在时间差小于或等于学习周期配置内属于机器学习周期，时间差大于学习周期配置属于非机器学习周期)内，针对步骤 A 解析还原后的原始行为，自动收集原始行为并提取特征，生成适应当前工业控制网络环境的白名单安全策

略规则（相当于基线形成模块，用于对采集的数据包进行预处理,将预处理后得到的数据作为训练数据集进行机器学习，生成适应当前工控环境的合法行为基线），步骤 C：在非机器学习周期内，针对解析工控系统中网络行为还原后的原始行为(即当前工控系统中网络行为还原后的原始行为，来进行网络审计和监测)，分别进行白名单安全策略规则检测，对于不符合白名单安全策略规则的原始行为，生成告警信息并记录其原始行为，便于事件回溯取证分析（相当于安全检测模块，用于根据所述合法行为基线在当前工控环境下进行安全检测，当检测到不符合所述基线形成模块学习的行为则告警），解析还原是基于端口来分析(Modbus、S7、IEC-104、DNP3、Ethernet/IP、MMS、FINS、OPC 等)常见的工控协议，并根据协议规范进行解析还原，获取所需信息，包括指令码、参数、响应码、原始行为；步骤 B：进行机器学习，即在机器学习周期(即指系统部署成功后，通过配置系统的机器学习周期，计算系统运行起始时间到系统当前时间的时间差，当系统运行在时间差小于或等于学习周期配置内属于机器学习周期，时间差大于学习周期配置属于非机器学习周期)内，针对步骤 A 解析还原后的原始行为，自动收集原始行为并提取特征，生成适应当前工业控制网络环境的白名单安全策略规则（相当于所述预处理模块，用于对所述数据采集模块采集的数据包进行预处理；所述机器学习模块，用于通过机器学习算法对所述预处理模块处理后得到的数据作为训练数据集进行机器学习；所述安全检测基线形成模块，用于根据所述机器学习模块的训练结果生成适应当前工控环境的合法行为基线）。可见，对比文件 1 公开了基于工业控制内部网部署安全探针装置，所述安全探针装置包括数据采集模块、基线形成模块和安全检测模块。

权利要求 1 请求保护的内容与对比文件 1 公开的内容相比较，可以确定其区别技术特征是：安全检测模块用于在不同公开环境下进行安全检测；所述预处理模块基于本体将数据聚合，即，将工业控制系统中具有相同概念和语义的数据进行归类和抽取，将聚合得到新的数据分类，所有分类构成的集合作为机器学习的训练数据集；所述机器学习模块基于 CNN/RNN 学习与建模；所述安全检测基线形成模块根据机器学习训练结果形成符合安全规范的协议特征、设备对象信息，并生成可供参考的网络通信特征列表，通过对协议分布和流量信息的匹配形成安全检测基线。经分析，其实际解决的技术问题是：如何进行不同工控环境下的安全检测。

对于上述区别技术特征：对比文件 1 公开了针对当前工控环境利用机器学习生成对应的行为基线，其相当于权利要求 1 中的基线形成模块，并且权利要求 1 中记载的是：生成适应当前工控环境的合法行为基线，而其实施过程中却是：根据所述合法行为基线在不同工控环境下进行安全检测。由于不同环境流量不同协议不同，生成的行为基线可能完全不适用，本领域技术人员有理由认为此处描述的行为基线包含了不同环境的学习结果，或者根据不同环境生成的不同的行为基线。因此在对比文件 1 的基础上，本领域技术人员能够想到上述两种可能用于不同工控环境下的安全检测方法。其中在基于机器学习的数据建模领域，常用的机器学习算法有 CNN/RNN 等，以及将相同概念和语义的数据进行归类和抽取，将其聚合成机器学习的训练数据

集属于本领域惯用技术手段；根据机器学习的训练结果形成特征表用作安全检测基准时，该特征表需要满足安全规范也属于本领域惯用技术手段，其中为了方便识别或记录检测结果相关的各种信息（比如是什么设备产生的异常行为），本领域技术人员能够想到在特征表中添加设备对象信息。

由此可见，在对比文件 1 的基础上结合本领域惯用技术手段，得到权利要求 1 请求保护的内容对于本领域技术人员来说是显而易见的，因此该权利要求不具备突出的实质性特点和显著的进步，因此该权利要求不具备专利法第 22 条第 3 款规定的创造性。

2.权利要求 2 不具备专利法第 22 条第 3 款规定的创造性。

权利要求 2 是权利要求 1 的从属权利要求，其进一步限定安全探针装置部署在主节点上。在计算机网络领域，为了便于管理或者隔离安全网段或者解决 IP 不足的问题，网络中存在不同的子网，但总的来说有一个主节点负责管理转发一个区域内所有的流量。因此为了针对某个工控环境的流量进行安全检测，本领域技术人员能够想到将安全探针装置部署在主节点上。因此，当其引用的权利要求不具备创造性时，该权利要求也不具备专利法第 22 条第 3 款规定的创造性。

3.权利要求 3 不具备专利法第 22 条第 3 款规定的创造性。

权利要求 3 是权利要求 1 的从属权利要求，对比文件 1 还公开了以下技术特征（参见说明书第[0036]段）：并根据协议规范进行解析还原，获取所需信息，包括指令码、参数、响应码、原始行为(相当于将所述数据包按照既定的通信协议规则解析出各个不同意义的字段，并将解析出来的每个字段的数据进行标记)。其中在计算机领域，本领域技术人员通过 PF_RING 进行数据包流量采集属于本领域惯用技术手段。因此，当其引用的权利要求不具备创造性时，该权利要求也不具备专利法第 22 条第 3 款规定的创造性。

4.权利要求 4 不具备专利法第 22 条第 3 款规定的创造性。

权利要求 4 是权利要求 1 的从属权利要求，其进一步限定构成其区别技术特征。在计算机安全领域，安全检测包括：实施应用白名单、配置合规性检查与补丁扫描、正常工控协议与异常工控协议列表等属于本领域惯用技术手段。因此，当其引用的权利要求不具备创造性时，该权利要求也不具备专利法第 22 条第 3 款规定的创造性。

5.权利要求 5 不具备专利法第 22 条第 3 款规定的创造性。

权利要求 5 是权利要求 4 的从属权利要求，在计算机安全领域，配置合规检测是通过对目标系统的配置文件进行解析，然后与符合安全标准的配置进行对比匹配以检测是否合规；其中符合安全标准的配置包括有具体业务操作、国家标准和行业标准等。因此，当其引用的权利要求不具备创造性时，该权利要求也不具备专利法第 22 条第 3 款规定的创造性。

6.权利要求 6 不具备专利法第 22 条第 3 款规定的创造性。

权利要求 6 是权利要求 5 的从属权利要求，对比文件 1 还公开了以下技术特征（参见说明书第[0057]

段）：流量采集模块使用 Libpcap 软件包进行网络数据包捕获，根据端口解析 Modbus、S7、IEC-104、DNP3、Ethernet/IP、MMS、FINS、OPC 等常见的工控协议，如 Modbus 协议默认 502 端口，S7 协议默认 102 端口，IEC-104 默认 2404 端口（相当于正常工控协议与异常工控协议列表针对不同行业工控网络进行异常监测；所述正常工控协议包括：DNP3、IEC104、、MODBUS、S7COMM），其中 IEC61850-GOOSE、IEC61850-MMS、IEC62351 等属于本领域惯用的工控协议，本领域技术人员在工控系统中使用到上述协议时，能够想到也针对上述协议进行异常监测。因此，当其引用的权利要求不具备创造性时，该权利要求也不具备专利法第 22 条第 3 款规定的创造性。

(二)、关于申请人的意见陈述

申请人认为：

对比文件 1 与本权 1 中的“所述预处理模块基于本体将数据聚合，即，将工业控制系统中具有相同概念和语义的数据进行归类和抽取，将聚合得到新的数据分类，所有分类构成的集合作为机器学习的训练数据集”不同，本权 1 公开了机器学习所需训练数据集的具体数据来源的预处理过程。

因此，本申请具备创造性。

对此，审查员有不同意见：

在工控环境中，由于不同环境流量不同协议不同，生成的行为基线可能完全不适用，本领域技术人员为了使得训练得到的模型能够适用于更多的环境，其训练过程包含了不同环境的学习结果，或者根据不同环境生成的不同的行为基线。因此在对比文件 1 的基础上，本领域技术人员能够想到上述两种可能用于不同工控环境下的安全检测方法，其中在第一种情况（训练的模型适用于更多环境）下，本领域技术人员在训练过程中需要将工业控制系统中具有相同概念和语义的数据进行归类和抽取，将聚合得到新的数据分类，所有分类构成的集合作为机器学习的训练数据集属于本领域管用技术手段，也即是为了得到适配更多环境的模型，需要对各个工控环境中的数据进行聚合处理，属于本领域惯用技术手段。

综上，申请人的意见陈述不成立。

三、决定

综上所述，本发明专利申请不符合专利法第 22 条第 3 款的规定，属于专利法实施细则第五十三条第二项的情况，因此根据专利法第三十八条予以驳回。

根据专利法第四十一条第一款的规定，申请人如果对本驳回决定不服，可以在收到本驳回决定之日起三个月内，向专利局复审和无效审理部请求复审。

审查员姓名:冉涛

审查员代码:30141733

纸件申请，回函请寄：100088 北京市海淀区蓟门桥西土城路 6 号　国家知识产权局专利局受理处收

电子申请，应当通过电子专利申请系统以电子文件形式提交相关文件。除另有规定外，以纸件等其他形式提交的文件视为未提交。