文章编号:1671-4598(2021)05-0040-05 DOI:10.16526/j.cnki.11—4762/tp.2021.05.008 中图分类号:TP301.6 文献标识码:A

大数据融合模型的智能化网络安全检测方法

王 鹏,胡宏彬,李 勇
(内蒙古电力科学研究院,呼和浩特 010010)

摘要:针对传统智能化网络安全检测平台处理数据效率低、误差大等问题,文章提出一种新型的解决方案;该方案基于大数据融合模型构建新型的智能化网络安全检测平台,采用卡尔曼滤波算法、采用数据融合分类算法和模糊推理算法3种方法结合构建出数据融合模型来对网络安全检测数据进行运算与处理;其中,采用卡尔曼滤波算法进行改进,对原始网络安全检测数据进行滤波降低噪声干扰,提高数据的精准度;通过SAE稀疏自动编码器自主提取网络安全检测数据的特征信息,之后K—means聚类算法对SAE稀疏自动编码器输出的数据进行处理,通过模糊推理算法调整权值;试验表明,文章所提方案克服了现有技术存在的不足,显著提高了处理数据效率和精准度,在数据量为2 TB的环境下,本研究方法的误差低至6.9%。

关键词:网络安全检测;大数据融合;噪声干扰;卡尔曼滤波;模糊推理

Intelligent Network Security Detection Method Based on Big Data Fusion Model

Wang Peng, Hu Hongbin, Li Yong
(Inner Mongolia Electric Power Research Institute, Hohhot 010010, China)

Abstract: Aiming at the problems of low data processing efficiency and large error of traditional intelligent network security monitoring platform, this paper proposes a new solution. The scheme builds a new intelligent network security monitoring platform based on the big data fusion model. It uses Kalman filter algorithm, data fusion classification algorithm and fuzzy reasoning algorithm to construct a data fusion model to calculate and process the network security monitoring data. Among them, Kalman filter algorithm is used to improve the original network security monitoring data to reduce noise interference and improve the accuracy of data; the feature information of network security monitoring data is extracted by SAE sparse automatic encoder, and then K—means clustering algorithm is used to process the output data of SAE sparse automatic encoder, and the weight is adjusted by fuzzy inference algorithm. The experimental results show that the proposed scheme overcomes the shortcomings of the existing technology and significantly improves the efficiency and accuracy of data processing. The error of this research method is as low as 6.9%.

Keywords: network security detection; big data fusion; noise interference; Kalman filter; fuzzy reasoning

0 引言

在信息智能化不断发展的时代,许多中小型企业的各种业务系统也在不断地更新与完善,所产生的数据也在迅猛地增长。产业互联网的迅速发展,带动了各行各业的生产水平,与此同时,智能网络时代也给企业的安全带来了全新的挑战[1]。互联网的负面作用正逐步扩大,网络安全问题成为了企业安全的重中之重,其中数据安全问题较为突出[2-3]。

针对上述存在的问题,许多学者发表了自己研究的技术方案。文献[4]公开了一种基于Hadoop平台卷积神经网络模型[4],虽然能在一定程度上对网络安全检测运算处理效果比较好,但是处理数据过程比较复杂导致效率低,对于实时数据无法快速处理。文献[5]提出了一种多源异构数据实时处理模型,采用了XML数据形式映射数据库的机制[5],虽然在实时数据处理上有明显的优势,但是采集的数据容易受到噪声干扰导致精度下降。本研究研究出一套适用的解决方案,下文将详述具体方案设计。

1 网络安全检测平台总体框架设计

针对上述技术存在的不足,本研究设计出新型的智能化网络安全检测平台,全面分析网络风险因素,以提高对网络风险因素的感知、预测和防范能力。本研究采用卡尔曼滤波算法、采用数据融合分类算法和模糊推理算法3种方法结合构建出数据融合模型来对网络安全检测数据进行运算与处理。关于网络安全检测平台总体框架图如图1所示。

如图1所示,网络安全检测平台总体框架可分为5大模块。

1)检测数据采集与预处理:

网络安全检测平台主要是通过物联网和企业的业务系

收稿日期:2020-09-29; **修回日期**:2020-10-26。
基金项目:内蒙古重大科技项目(NMG2020JG0091)。
作者简介:王 鹏(1988-),男,内蒙古呼和浩特人,硕士,工程师,主要从事网络安全、大数据、区块链方向的研究。
引用格式:王 鹏,胡宏彬,李 勇.大数据融合模型的智能化网络安全检测方法[J].计算机测量与控制,2021,29(5):40-44.

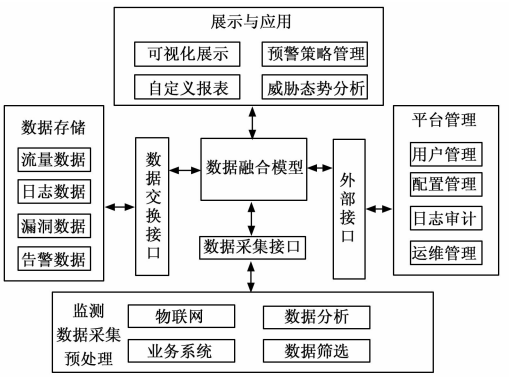

图 1　网络安全检测平台总体框架图

统中获取数据，利用网络采集探针在关键网络节点进行实时检测。采集内容应该包括网络流量、日志、系统漏洞和各个业务系统之间交互数据等信息，在原始流量中经过分析得出已知威胁，将数据进行预处理之后通过数据采集接口传输至数据融合模型之中进一步进行数据处理[6-7]。

2）数据存储：

数据存储主要是将采集得到的不同结构的数据进行合理地存储，与数据融合模型通过数据交互接口进行信息交互，便于数据融合模型的运算。

3）平台管理：

包括平台的管理、数据存储以及自身安全防护，通过实时监控来主动发现安全漏洞并及时预警，充分运维管理网络安全检测平台，加强全网安全形势意识和安全监控，为平台的总体功能实现提供支撑。

4）数据融合模型：

在本研究的数据融合模型中，在结构上分为卡尔曼滤波算法、采用数据融合分类算法和模糊推理算法，采用多种算法能将复杂的网络安全检测大数据进行融合处理产生最优权重值提高了数据有效性，提高了网络应用效率。最终将处理结果传达至展示与应用模块。

5）展示与应用：

在对显示单元中存在的隐藏数据信息中，依据决策者、管理人员和运维人员对网络应用安全的需求侧重点，利用可视化分析技术，进行多种态势的多维度展示，并且支持预警通告和应急处置[8]。

2　数据融合模型的构建

在对复杂的网络安全检测大数据处理方面，通常是采用数据融合技术来将不同结构的网络安全检测数据进行互补优化，得到更好的数据结果。本研究设计了网络安全检测数据融合组合算法模型，采用多种算法将复杂的网络安全检测大数据进行融合处理产生最优权重值提高了数据有效性和网络利用率。关于数据融合模型如图 2 所示。

结合图 2 对网络安全检测数据融合模型进行说明。在结构原理上，首先应用卡尔曼滤波算法进行数据融合处理，以提高数据的纯度，进而提高计算的精度。其次采用数据融合分类算法为对网络安全检测数据进行进一步的关联融合，通过稀疏自编码器进行自主提取数据特征。为了进行数据聚类，通过 K－means 聚类算法模型对接收到的数据进行聚类处理，并通过 softmax 函数输出分类器，进而实现多种数据的融合计算和处理；最后将处理后的数据信息输出至模糊推理算法，对接收到的网络安全检测数据从整体上进行性能评估。

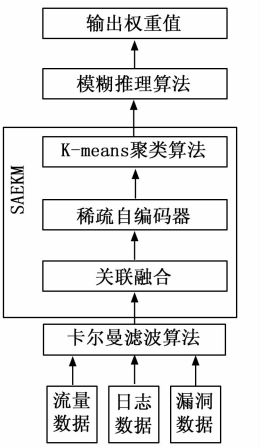

图 2　网络安全检测数据融合模型

2.1　卡尔曼滤波算法

在实际网络采集探针在关键网络节点进行实时检测过程中，采集过程和传输过程的周边环境难免会受到各种外界因素的干扰。为了降低噪声干扰提高数据的准确度，本研究将卡尔曼滤波算法进行了新型的应用，在应用过程中对原始网络安全检测数据进行初始化滤波处理[9]。计算方法的详解如下文所示：

针对关键网络节点处首先建立状态方程和量测方程为：

$$\begin{cases} x_{k+1} = \boldsymbol{A}_k x_k + w_k \\ y_k = \boldsymbol{H}_k x_k + v_k \end{cases} \tag{1}$$

式（1）中，k 表示某一时刻，取不为 0 的自然数；x_k 表示在 k 时刻网络安全检测信号的状态变量，y_k 分别表示在 k 时刻网络安全检测信号的量测变量；$\boldsymbol{A}_k$ 和 $\boldsymbol{H}_k$ 分别表示在 k 时刻网络安全检测信号的状态转移矩阵和量测系数矩阵；W_k 和 V_k 分别表示在 k 时刻网络安全检测信号的动态噪声和量测噪声。

其次，根据式（1）建立误差初始化方程为：

$$\begin{cases} x(0 \mid 0) = E(x_0) \\ P_x(0 \mid 0) = E[(x_0 - x(0 \mid 0))(x_0 - x(0 \mid 0))^T] \end{cases} \tag{2}$$

式（2）中，P 为计算误差初始化方程中对应 x 的协方差，E 为计算的误差值。经过卡尔曼滤波递推，得到：

$$\begin{cases} x(k \mid k-1) = \boldsymbol{A}_k x(k-1 \mid k-1) \\ P_x(k \mid k-1) = \boldsymbol{A}_k P_x(k-1 \mid k-1) \boldsymbol{A}_k{}^T \end{cases} \tag{3}$$

$$J_k = \frac{P_x(k \mid k-1)}{\boldsymbol{H}_k P_x(k \mid k-1) \boldsymbol{H}_k{}^T + R_v(k)} \tag{4}$$

$$Q_w = E[w_k w_k{}^T] R_v = E[v_k v_k{}^T] \tag{5}$$

其中：Q 和 R 分别表示在 k 时刻网络安全检测信号的

动态噪声和量测噪声各自的协方差；J 表示最终运算的滤波值。

综上式（1）～（5）[10-11]可以看出，卡尔曼滤波算法过程是一个迭代过程，当得到新的网络安全检测数据时，即可算出新的滤波值，实现对原始网络安全检测数据的降噪处理。

2.2 数据融合分类算法

本研究的数据融合分类算法是在 K－means 聚类的稀疏自动编码器融合算法的基础上，应用 SAE 稀疏自动编码器将网络安全检测数据的特征信息自主地提取出来，然后启动 K－means 聚类算法模型接收上述数据信息，对 SAE 稀疏自动编码器输出的数据进行处理[12-13]。关于数据融合分类算法的具体步骤如下：

1）设 3 种不同结构网络安全检测数据集 $A=\{a_1, a_2, \cdots, a_N\}$，$B=\{b_1, b_2\cdots, b_N\}$，$C=\{c_1, c_2, \cdots, c_N\}$ 均含有 N 个样本，经过关联融合后得到数据样本集[14-15] $D=\{a_1, a_2, \cdots, a_N, b_1, b_2\cdots, b_N, c_1, c_2, \cdots, c_N\}$。

2）通过 SAE 稀疏自动编码器建立 3 个隐藏层，本研究构建三次神经网络模型来提取网络安全检测数据的特征信息。构建 SAE 稀疏自动编码器网络模型主要通过编码和解码过程。在编码过程中，提取隐藏层特征第 k 个网络安全检测数据样本编码公式为[16-17]：

$$\begin{aligned} a_k &= f_\theta(d_k) = f(T_1 d_k + C_1) \\ b_k &= f_\theta(d_k) = f(T_1 d_k + C_1) \\ c_k &= f_\theta(d_k) = f(T_1 d_k + C_1) \end{aligned} \tag{6}$$

式（1）中，$f(x)$ 为激活函数，θ 为 SAE 稀疏自动编码器的参数。通常编码和解码过程常用的激活函数为 ReLU 函数和 sigmoid 函数，本研究在编码过程中使用 ReLU 函数，而在解码过程中将两种激活函数混合使用[18]。

在解码过程中，将对网络安全检测数据进行重构，得到与输入层的原始网络安全检测数据最接近的输出量 g_k，如公式（7）所示[19]：

$$\begin{aligned} g_k &= f_\theta(x) = f(T_2 x + C_2) \\ x &= a_k, b_k, c_k \end{aligned} \tag{7}$$

其中：x 为 3 种网络安全检测数据集任意一种，$T_1=T_2{}^T$，$C_1=C_2{}^T$。

3）对网络安全相关数据进行设置，比如网络硬件参数、损失函数和优化器。神经网络模型参数主要由迭代次数、批处理以及学习速率组成，损失函数则通过调用 PyTorch 数据库内的均方损失函数 MSELoss，在模型中为了防止数据出现过拟合现象，本研究采用 Adam 优化器对数据进行优化[19-20]。关于具体实现程序相关代码如下[21]：

迭代次数：nmm_epochs＝200

批处理个数：batch_size＝1280

学习速率：lerning_rate＝1e－3

采用 Adam 优化器：

optimizer＝torch. optim. Adam(model. parameters(),lr＝learning_rate weight_decay＝1e－5)

设置均方损失函数：criterion＝nn. MSELoss

最后一步，通过 SAE 稀疏自动编码器输出量作为 K－means 聚类算法的输入量。首先要先确立一个输入网络安全检测数据的中心点；其次每个网络安全检测数据点通过 ou _ distance 函数来定义数据点与所设中心点之间的欧式距离；然后通过分析计算距离所设中心点最近的数据点，确定该点归属于哪一种网络安全检测数据类别。最后，计算中心点与所有其他数据点之间的距离之和，并计算每类网络安全检测数据集中每个点与所有其他点之间的距离之和。如果距离小于当前中心点之和，则删除中心点并再次分割质心。经过多次循环，得到最终的分类结果[22]。

2.3 模糊推理算法

通过模糊推理算法对数据融合分类算法的结果进行数据融合，根据结果决定是否调整权值，并将调整后的权值隐含在其权值矩阵中，使数据融合更加适宜。关于具体步骤如下[23]：

（1）对输入量进行量化，假设模糊推理结果为 F，数据融合分类算法结果为 U_1，卡尔曼滤波算法结果为 U_2。

（2）从专家级研究经验进行推理分析，得出模糊推理结果 F 的定义式为：

$$F = F_i \mid i \in M, F_i = [0,1]\begin{bmatrix} U_1 \\ U_2 \end{bmatrix} \tag{8}$$

其中：i 是某个网络安全检测数据样本，M 是总网络安全检测数据样本集合，当 F_i 趋近于 0 时，说明网络安全检测数据损失值小，表明融合性好；当 F_i 趋近于 1 时，说明网络安全检测数据损失值大，表明融合性差。

3 实验与分析

为了验证本研究设计的数据融合模型的适用性与可靠性，下面进行实验。

3.1 实验环境与数据样本

关于实验硬件环境为 Pentium（R）CPU、8 核 16G 内存，电脑的硬盘容量为 512G 的硬件环境，软件的操作系统 Windows10，JDK5.0，通过 MATLAB 软件系统进行仿真。

本研究以某企业近五年来受到网络安全威胁情报作为数据样本对象，对每条告警日志进行处理与分析，重点关注源 IP 地址、目的 IP 地址、动作等字段，分析清楚每个字段的含义，之后提取威胁 IP 地址进行进一步的评估。关于网络安全检测数据样本某个告警日志重要字段说明如表 1 所示。

通过输入威胁 IP 地址输出此威胁的评估值，由上级管理决定是否采取相应措施，从而消除网络安全威胁。

3.2 实验内容与结果分析

为了验证本研究所设计的数据融合模型的优势，本研究以卷积神经网络（CNN）方法和交叉映射（CM）方法作为对比，采用不同方法计算 0～2TB 网络安全检测数据量范围内融合损失值。在以下实验中，本研究所采用的卡尔曼滤波算法参数 $Q=10^{-6}$，$R=10^{-1}$。通过 MATLAB 软件系统进行仿真对比，对比结果图如图 3 所示。

表 1　重要字段说明

序号	名称	字段
1	时间	2019/7/4 8:46
2	协议	TCP. HTTP
3	恶意程序 ID	S_httptool_Rsas
4	客户端 IP	202.96.14.222
5	客户端端口	50047
6	客户端 MAC 地址	00:0D:48:2A:21:59
7	服务器 IP	124.192.164.35
8	服务器端口	80
9	进包数	5
10	进流量	1.007 kB
11	出包数	4
12	出流量	837 byte

如图 3 所示，本研究所采用的数据融合模型方法比 CNN 算法和 CM 算法的损失值更低，网络安全检测数据融合性更好。因此得出结论，本研究的数据融合模型更加适用。

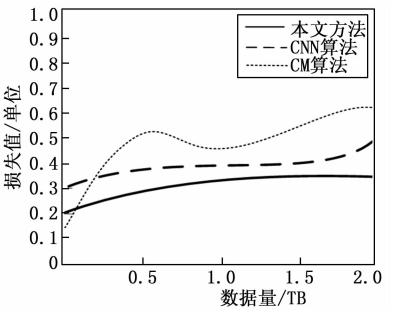

图 3　损失值对比结果图

为了进一步验证本研究的数据融合模型高精度和低能耗的优点，采用不同方法计算 0～2 TB 网络安全检测数据量范围内误差率和网络节点平均剩余能量，得出结果进行对比如图 4 和表 2 所示。

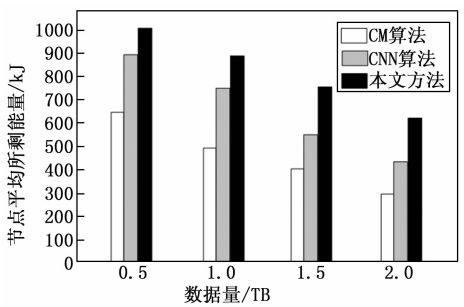

图 4　节点平均剩余能量对比结果图

表 2　3 种方法误差对比结果

数据量/TB	误差/%		
	本研究方法	CNN 算法	CM 算法
0.5	5.2	6.7	9.4
1.0	5.6	7.8	9.6
1.5	6.1	8.3	9.8
2.0	6.9	9.0	9.9

通过对图 4 和表 2 中的结果分析，本研究本研究的数据融合模型不仅误差数值最低，而且由于运算过程效率高使得网络节点能耗较低。因此得出结论，本研究数据融合模型可靠性要更高。

4　结束语

结合新时代智能化网络背景下对企业网络安全保护的需求，本研究设计出新型的智能化网络安全检测平台，在数据传输的过程中利用数据融合技术对网络中的数据进行融合处理，采用卡尔曼滤波算法提高网络安全检测数据的精准度。通过分析存在的威胁和漏洞，评估网络威胁带来的危害程度，最后利用某企业的告警日志数据通过实验验证了本研究网络安全检测数据融合模型的适用性和可靠性。结果表明，该改进算法产生最优估计值提高了数据有效性，处理后的数据传输降低了网络能耗。随着技术的不断发展，对于智能化网络安全检测平台采集精准度和全面性要求会更高，本研究仍旧存在诸多不足，有待进一步的研究。

参考文献：

[1] 贺雅琪. 多源异构数据融合关键技术研究及其应用 [D]. 成都：电子科技大学，2018.

[2] 林丽丹，李　娜. 大数据技术在高校智慧校园建设中的应用研究 [J]. 电脑知识与技术，2020，16 (18)：36－28.

[3] Zhang Y，Wang Y，Ding H，et al. Deep well construction of big data platform based on multi－source heterogeneous data fusion [J]. International Journal of Internet Manufacturing and Services，2019，6 (4)：371－388.

[4] 华　钢，曹青峰，朱艾春，等. 多流卷积神经网络的骨架行为识别 [J]. 小型微型计算机系统，2020，41 (6)：1286－1290.

[5] 李　亢，李　一，刘　东. 多源异构装备数据集成研究综述 [J]. 中国电子科学研究院学报，2015，10 (2)：162－168.

[6] 杨　柳，于　剑，刘　烨，等. 面向认知的多源数据学习理论和算法研究进展 [J]. 软件学报，2017，28 (11)：2971－2991.

[7] 陶永才，张鑫倩，石　磊，等. 面向短文本情感分析的多特征融合方法研究 [J]. 小型微型计算机系统，2020，41 (6)：1126－1132.

[8] 金　丰，邵　清. 信号分解与融合神经网络的金融数据预测研究 [J]. 小型微型计算机系统，2020，41 (6)：1140－1146.

[9] 邓洪明，贺　勇，刘立辉. 无人机数据采集 EKF 滤波悬停稳定的研究与应用 [J]. 计算机测量与控制，2018，26 (3)：180－182.

[10] 魏克新，陈峭岩. 基于自适应无迹卡尔曼滤波算法的锂离子动力电池状态估计 [J]. 中国电机工程学报，2014，34 (3)：445－452.

[11] Machida S，Miyashita Y，Ieda A，et al. Statistical visualization of the Earth’s magneto tail and the implied mechanism of sub storm triggering based on superposed epoch analysis of THEMIS data [J]. Annales Geophysicae，2014，32 (2)：99－111.

[12] 张　军，杨子晨. 多传感器数据采集系统中的数据融合研究

[J]. 传感器与微系统，2014，33 (3)：52－54.
[13] 吕红芳，顾幸生. 基于蚁群神经网络的两级信息融合算法 [J]. 上海交通大学学报，2016，50 (8)：1323－1330.
[14] 王 力. 基于 DS 证据理论的多传感器数据融合算法研究与应用 [D]. 太原：太原理工大学，2015.
[15] 陈 前. 基于数据融合的通信机房环境监控无线传感网络设计与实现 [D]. 重庆：重庆大学，2014.
[16] 孙田川，刘洁瑜. 基于支持度和自适应加权的 MEMS 陀螺信息融合算法 [J]. 传感技术学报，2016，29 (10)：1548－1552.
[17] 阎 博，张 昊，郭子明，等. 基于多源数据融合的电网故障综合分析与智能告警技术研究与应用 [J]. 中国电力，2018，51 (2)：39－46.
[18] 祁 波，孙书利. 带未知通信干扰和丢包补偿的多传感器网络化不确定系统的分布式融合滤波 [J]. 自动化学报，2018，44 (6)：1107－1114.
[19] 杨启京，张 勇，翟明玉，等. 大电网未来态一体化模型构建和融合技术研究 [J]. 中国电力，2018，51 (6)：121－128.
[20] 王 惠，刘 霓，刘东全. 政务部门网络安全态势感知系统构建研究 [J]. 中国信息安全，2019，111 (3)：80－81.
[21] 杨 安，孙利民，王小山，等. 工业控制系统入侵检测技术综述 [J]. 计算机研究与发展，2016，53 (9)：2039－2054.
[22] 赖英旭，刘增辉，蔡晓田，等. 工业控制系统入侵检测研究综述 [J]. 通信学报，2017，38 (2)：143－156.
[23] 钱 伟，何志祥，张德银. 基于模糊神经网络的火灾传感器特征参数融合算法 [J]. 传感技术学报，2017，30 (12)：1906－1911.

(上接第 33 页)

1) 驱动器 IO 口故障定位：

自动准直组件进入第三年运行以后，某区域的驱动模块的限位开关 IO 口陆续出现失效的问题。根据历史故障记录分析对比不同束组出现的的限位开关故障，先投入运行的束组控制系统出现 IO 口故障频率越高，也就是故障的频率与运行时间呈正比，貌似与器件老化相关。但是对比单个束组不同区域的 IO 口故障，故障区域的 IO 口故障整体偏高。进一步分析驱动模块的 IO 口信号，IO 口故障通常发生在电信号下降沿，工作在常闭状态下的 IO 口故障率远远大于工作在常开工作状态的 IO 口。对多个 IO 口的工作电流进行监测，发现常闭状态 IO 口的工作电流为 12 毫安，远大于产品手册要求的 5 毫安，可能时导致 IO 口非正常老化的根本原因。在不同束组上进行增加限流电阻、不增加限流电阻两种技术手段的对比试验，统计 3 个月之后的累计故障，增加限流电阻可以有效的避免 IO 口故障发生，由此判断 IO 口工作电流大是导致此区域 IO 口异常老化损坏的根本原因。

2) 通讯模块故障分析：

通讯模块在近两年的运行中故障率较高。分析通讯模块的近两年的故障历史记录，发现通讯模块的故障时间与控制器状态变化时间强相关。在历史趋势曲线中分析通讯模块故障状态位和控制器状态位的时序，发现通讯模块故障通常发生在控制器启动后进入运行状态的时刻，此时也是 EtherCAT 通讯网络首次自检的时刻，由此确定通讯模块的故障可能与控制器启动时的电源干扰相关。采用电源隔离解决了部分通讯模块故障问题，对于不能进行硬件改造的通讯模块，减少系统启动次数，当检测到通讯模块故障后重新启动也能有效的减少通讯模块故障的发生频率。

利用运动控制状态监测系统的状态、故障历史数据，通过回溯分析工具，能够有效的分析、发现故障，保障主放大准直控制组件的长期稳定运行。

5 结束语

针对激光装置主放大自动准直组件，基于 KingSCADA 组态软件，研制了运动控制状态监测系统，实现了运动控制系统部件的状态监测、数据归档、趋势和报警显示，提升了运动控制系统的在线诊断和分析能力，为运动控制系统的故障诊断提供基础分析数据。

目前运动控制状态监测系统的数据分析能力有限，仅能进行单变量的统计分析，通过后续历史数据库的建设完善，采用关联数据分析算法，能够进一步提升控制系统的智能故障诊断能力。

参考文献：

[1] 李 红，朱健强，林 强，等. 高功率激光装置快速自动准直系统 [J]. 光子学报，2017 (10)：8－14.
[2] 周 维，胡东霞，赵军普，等. 高功率固体激光器光路自动准直算法与流程优化 [J]. 中国激光，2010 (1)：78－81.
[3] 高妍琦，朱宝强，刘代中，等. 四程放大自动准直系统数学模型研究 [J]. 物理学报，2008 (11)：6992－6997.
[4] 申立琴，马彩文，田新锋，等. 倍福 Beckhoff 在步进电机控制中的应用 [J]. 现代电子技术，2008 (21)：127－129.
[5] 邵忠喜，付云忠，富宏亚，等. 终端光学组件及反射镜架控制系统的开发 [J]. 哈尔滨工业大学学报，2013 (1)：67－71.
[6] 马国华，监控组态软件及其应所有 [M]，北京：清华大学出版社.
[7] 欧金成，欧世乐，林德杰，等. 组态软件的现状与发展 [J]. 工业控制计算机，2002 (4)：1－4.
[8] 亚控公司. KingSCADA 用户手册 V3.51 [Z]. 2015.
[9] 亚控科技. 基于 KingIOServer 的智能楼宇系统建设解决方案 [J]. 自动化博览，2018 (10)：52－55.
[10] 朱里红，杨 明，王 洋. 基于信息化平台的焦炉集气管压力监控系统的开发 [J]. 电气自动化，2014 (3)：26－28.
[11] 宋 元，吴勇航，翁 璐，等. 基于 InTouch 的风洞自主式维修保障系统监控软件设计 [J]. 计算机测量与控制，2015 (12)：4229－4231.