目录

第一章 软件概述

随着信息技术的大量渗入，现代电力系统已经发展成为由电力及其监控系统构成的复杂信息-物理系统（Cyber-Physical System，CPS），面临着愈加严重的信息物理安全问题，而恶意数据注入攻击问题是其中一种重要的形式。基于电压源型换流器的高压直流输电（Voltage Source Converter based High Voltage Direct Current Transmission，VSC-HVDC）系统作为现代电网的重要组成部分，其所面临的恶意数据注入攻击问题对 VSC-HVDC 系统自身甚至整个交直流系统的安全稳定运行具有重要影响。

目前，业界仍无对 VSC-HVDC 系统恶意数据注入攻击的研究，且电网运行人员对 VSC-HVDC 系统所面临的恶意数据注入攻击问题也没有足够的认识。因此，电力系统迫切需要一套能够帮助电网运行人员认识和分析 VSC-HVDC 系统恶意数据注入攻击问题的软件，提高电网运行人员对此类攻击问题的防范意识。

VSC-HVDC 系统恶意数据注入攻击演示与分析软件通过求解以破坏电网中 VSC-HVDC 系统换流器安全运行为目标的恶意数据注入攻击策略模型，向用户演示 VSC-HVDC 系统面临的恶意数据注入攻击问题。对于数据量较大的交流系统数据，用户可选择输入 BPA 标准格式的数据，大大减小了实际电网用户使用该软件时转化数据的工作量。通过表格或者图形展示输入的系统数据和计算结果，大大增强了软件的可视化效果。此外，软件的批量分析功能可分析恶意数据注入攻击对状态估计中最大标准化残差的影响，从而进一步分析攻击的成功率。

第二章 软硬件环境及设计流程

2.1 软件开发环境

本软件采用 Python 语言和 XML 语言作为编程语言。

本软件是在 Python 2.7 开发环境和 Qt Desigher 下完成的。

2.2 软件使用环境

本软件可在 Windows 7 操作平台上运行，内存要求在 1GB 以上。另外，要求运行环境下具有 IPOPT 程序的可执行文件 ipopt.exe，并将 ipopt.exe 所在的路径加入操作系统的环境变量中。

2.3 软件功能描述

软件的主要功能是读取包括交流系统数据、VSC-HVDC 系统数据、量测配置数据和节点地理位置数据在内的系统数据，求解以攻击 VSC-HVDC 系统换流器运行安全为目标的恶意数据注入攻击策略模型，并向用户演示攻击前后状态估

计中量测量的标准化残差、被攻击换流器的 P-Q 运行极限图以及运行点，同时给出需要篡改的量测量的值。此外，软件还具有批量分析功能，分析恶意数据注入攻击对状态估计中最大标准化残差的影响和攻击的成功率。软件设计中主要功能的详细说明如下：

1. 状态估计模块

软件的状态估计模块通过求解以下的优化模型得到系统状态变量的估计值 $\hat{\boldsymbol{x}}$，即：

$$\hat{\boldsymbol{x}} = \arg\min_{\boldsymbol{x}} \left[\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})\right]^T \boldsymbol{R}^{-1} \left[\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})\right]$$

其中，$\boldsymbol{R}$ 为量测向量 $\boldsymbol{z}$ 的误差方差矩阵，$\boldsymbol{h}(\boldsymbol{x})$ 表示量测方程。

2. 残差分析模块

软件的残差分析模块按照下式计算状态估计后各量测量的标准化残差，若恶意数据注入攻击后各量测量标准化残差的最大值未超过给定的阈值，说明恶意数据注入攻击能够躲过状态估计的不良数据检测环节，即恶意数据注入攻击成功：

$$r_i^N = \frac{\left|z_i - h_i(\hat{\boldsymbol{x}})\right|}{\sqrt{\Omega_{ii}}}$$

其中，$\boldsymbol{\Omega}$ 表示残差协方差矩阵。

3. P-Q 运行图模块

为保证换流器的安全运行，VSC-HVDC 系统的稳态运行点必须位 P-Q 运行极限图的安全运行区间，以保证流入换流器的交流侧电流幅值和交流侧电压幅值均小于一定的限值。

如图 1 所示，P-Q 运行极限图的安全运行区间为两个运行极限圆的交叉区域，其中，实线圆反映了流入换流器的交流侧电流幅值限制，假设允许流入换流器的最大交流侧电流幅值为 $I_{c1,\max}$，则该圆的圆心位于原点，半径为 $U_{s1}I_{c1,\max}$；另外虚线圆反映了换流器交流侧电压幅值限制，假设换流器允许的最大交流侧电压幅值为 $U_{c1,\max}$，虚线圆弧所在圆的圆心为 $(-U_{s1}{}^2 g_{tc1}, U_{s1}{}^2 b_{tc1})$，半径为 $U_{s1}U_{c1,\max}|y_{tc1}|$，其中 $y_{tc1} = g_{tc1} + \mathrm{j}b_{tc1}$ 表示换流电抗器 y_{c1} 和换流变压器 y_{t1} 串联后的等效导纳。

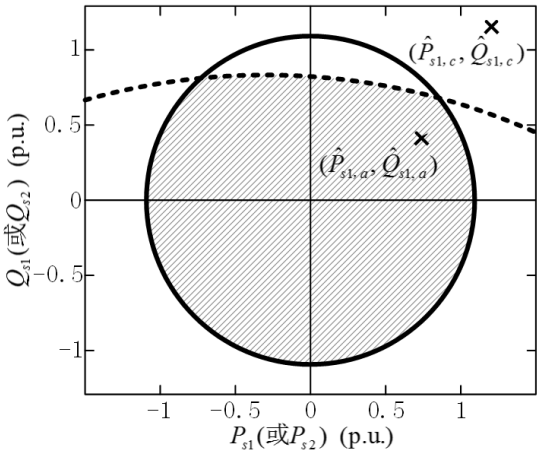

图 1 VSC-HVDC 系统换流器 P-Q 运行极限图

4. 恶意数据注入攻击模块

软件中利用的针对 VSC-HVDC 系统的恶意数据注入攻击策略模型如下：

$$\boldsymbol{z}_a = \arg\min_{\boldsymbol{z}} \left\| \boldsymbol{z} - \boldsymbol{z}_c \right\|_0$$

$$\text{s.t.} \begin{cases} \boldsymbol{z} = \underline{\boldsymbol{z}} + \boldsymbol{e} + \boldsymbol{b} \\ \underline{\boldsymbol{z}} = \boldsymbol{h}(\underline{\boldsymbol{x}}) \\ \hat{\boldsymbol{x}} = f_{SE}(\boldsymbol{z}) \\ \hat{\boldsymbol{z}}' = \boldsymbol{h}'(\hat{\boldsymbol{x}}) \\ \hat{P}_{s1}^{\,2} + \hat{Q}_{s1}^{\,2} \le \left(r_1 \hat{U}_{s1} I_{c1,\max} \right)^2 \\ \left(\hat{P}_{s1} + \hat{U}_{s1}^{\,2} g_{tc1} \right)^2 + \left(\hat{Q}_{s1} - \hat{U}_{s1}^{\,2} b_{tc1} \right)^2 \\ \le \left(r_2 \hat{U}_{s1} U_{c1,\max} |y_{tc1}| \right)^2 \\ \boldsymbol{x}_{\min} \le \hat{\boldsymbol{x}} \le \boldsymbol{x}_{\max} \end{cases}$$

其中，$\|\bullet\|_0$ 表示向量的 L0 范数；r_1、r_2 为给定的系数，且满足 r_1(或r_2)≤ 1，当 VSC-HVDC 系统运行中留有一定安全裕度时，其取值需适当减小；$\boldsymbol{x}_{\min}$ 和 $\boldsymbol{x}_{\max}$ 分别表示系统正常运行状态下状态向量的最小值向量和最大值向量。

本软件的整体应用流程如下图所示：

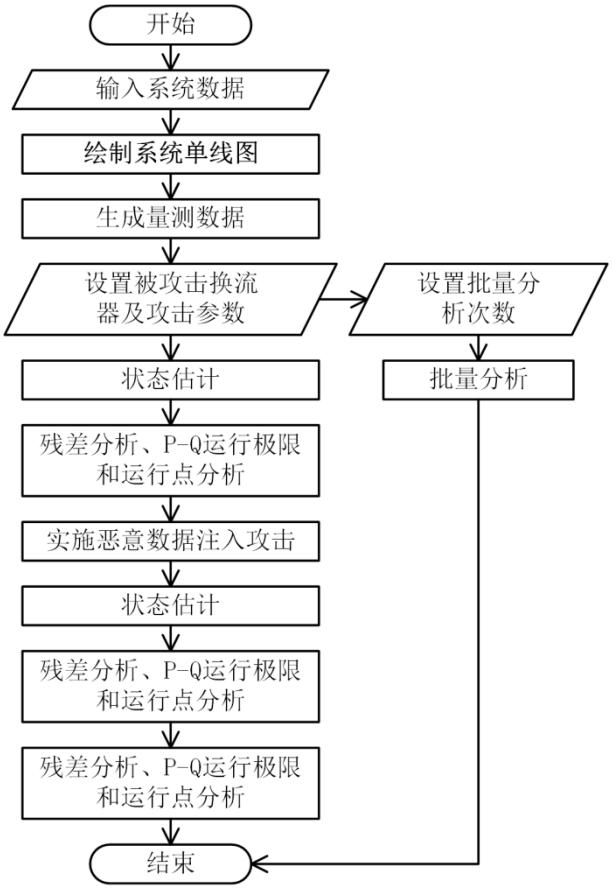

图 2 软件整体流程图

第三章 软件操作说明

3.1 软件基本操作

双击运行本软件，进入软件的主界面，如图 3 所示。主界面由两个子界面组成，左侧界面用于系统数据导入和数据查看，右侧界面用于执行程序功能和展示计算分析结果。可通过拖动子界面将其从主界面中脱离出来，如图 4 和图 5 所示。程序运行完成后点击界面右上侧的“退出”按钮可退出程序。

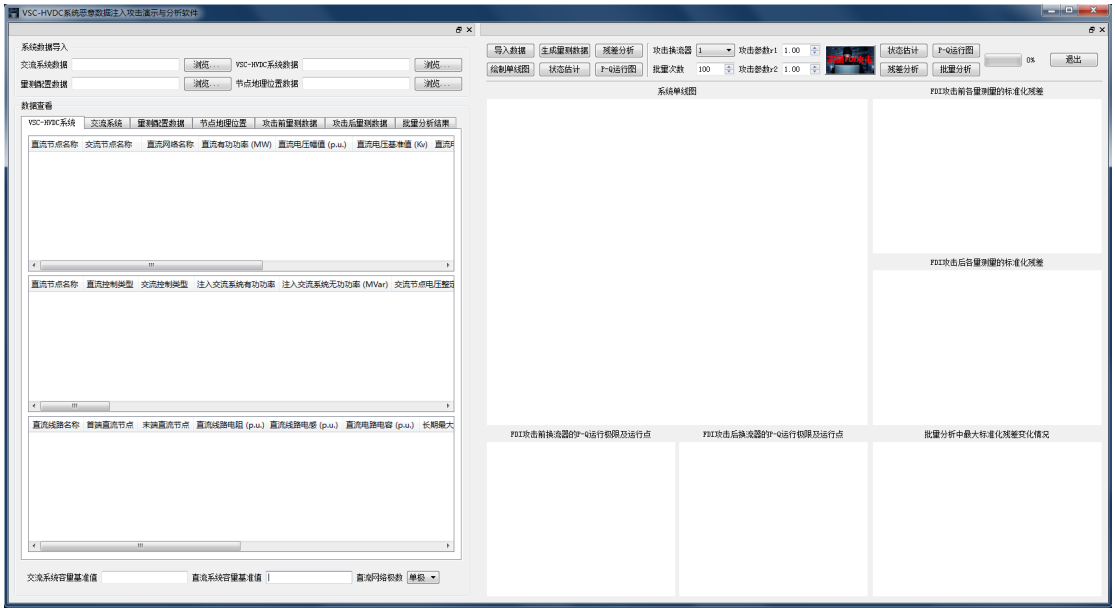

图 3

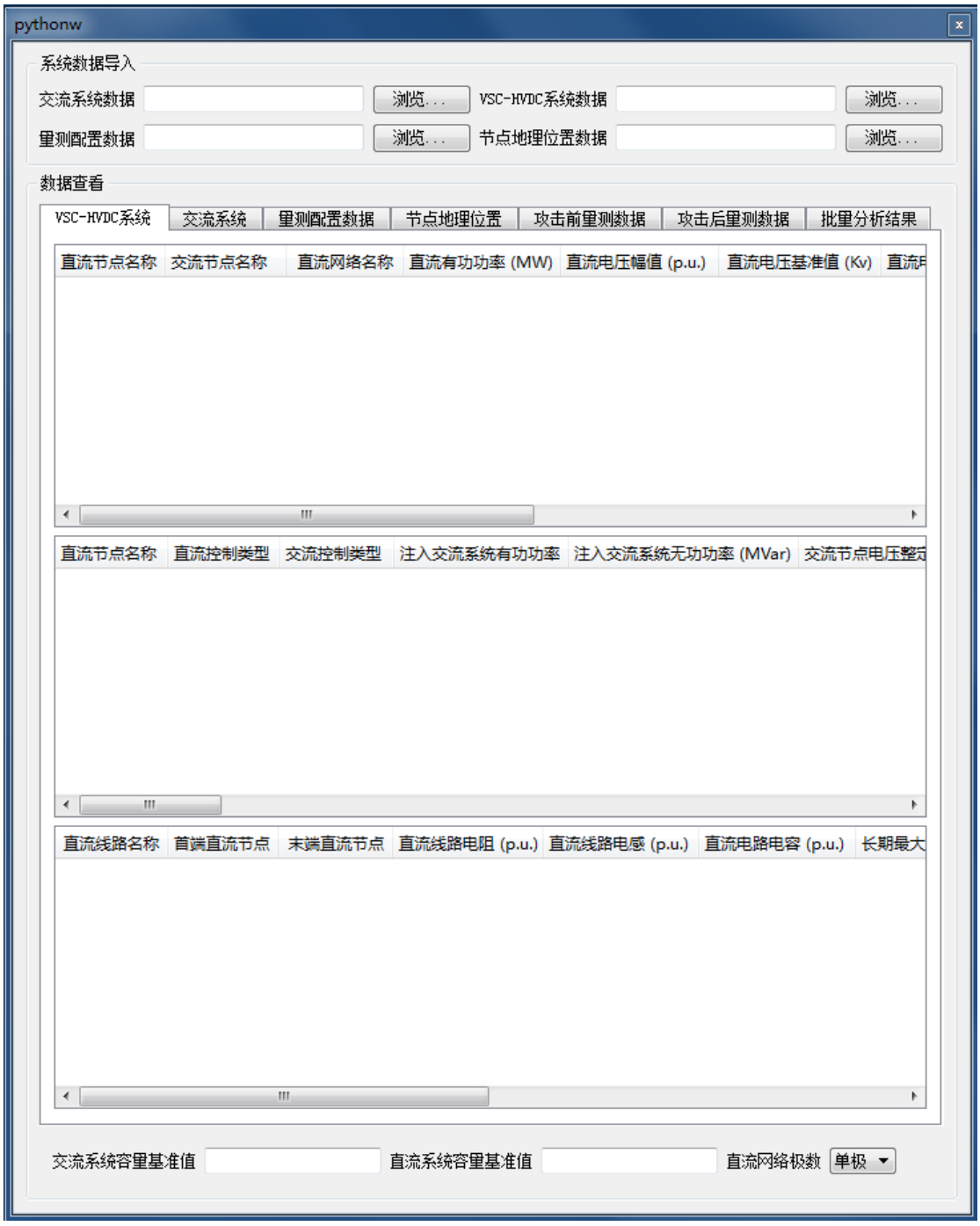
pythonw
系统数据导入
交流系统数据
浏览...
VSC-HVDC系统数据
浏览...
量测配置数据
浏览...
节点地理位置数据
浏览...
数据查看
VSC-HVDC系统
交流系统
量测配置数据
节点地理位置
攻击前量测数据
攻击后量测数据
批量分析结果
直流节点名称
交流节点名称
直流网络名称
直流有功功率 (MW)
直流电压幅值 (p.u.)
直流电压基准值 (Kv)
直流节点名称
直流控制类型
交流控制类型
注入交流系统有功功率
注入交流系统无功功率 (MVar)
交流节点电压整定
直流线路名称
首端直流节点
末端直流节点
直流线路电阻 (p.u.)
直流线路电感 (p.u.)
直流电路电容 (p.u.)
长期最大
交流系统容量基准值
直流系统容量基准值
直流网络极数
单极

图 4

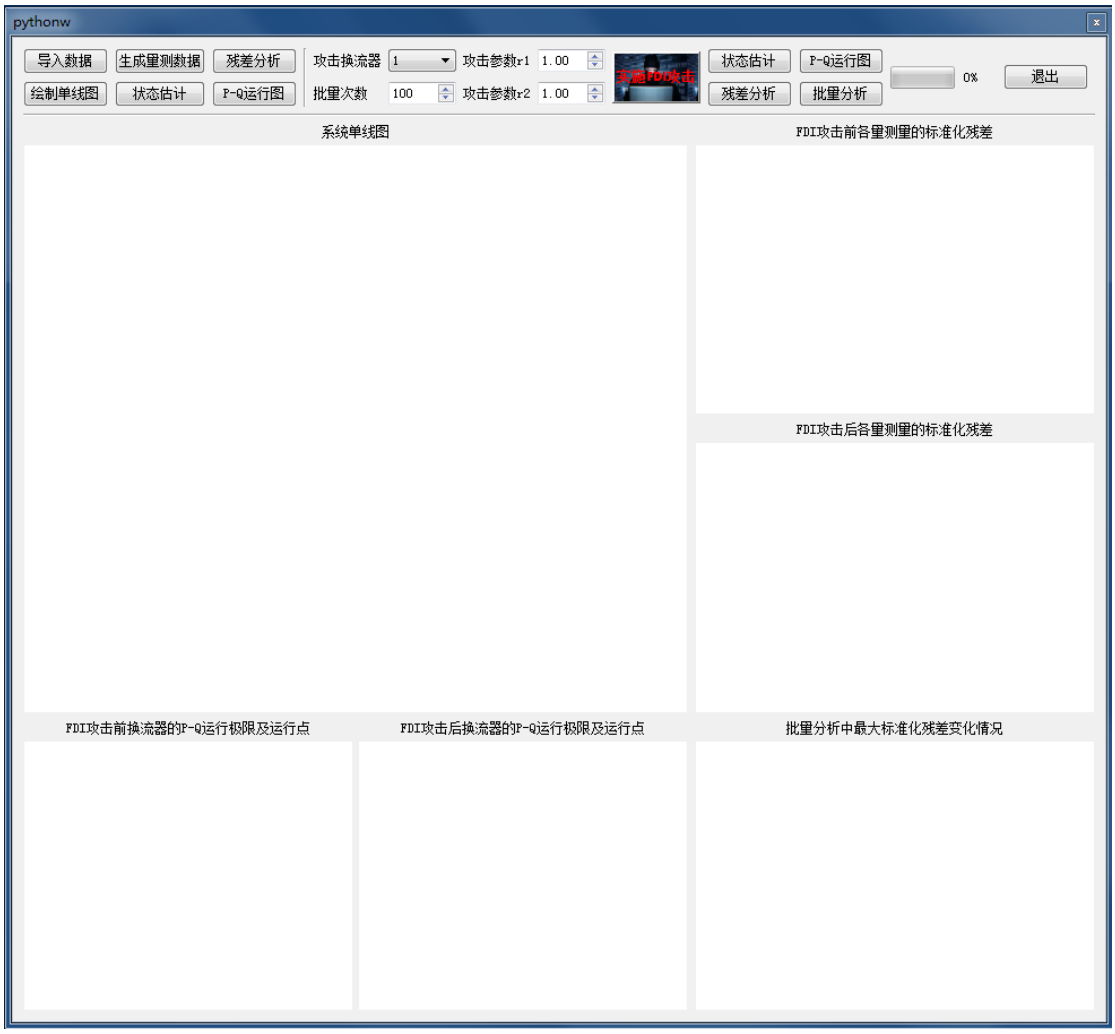

图 5

3.2 系统数据导入

通过界面中图 6 所示的系统数据导入模块选择系统数据文件所在路径，点击软件中的“导入数据”按钮，可将所选路径下的文件导入程序，并展示在软件的数据查看部分，如图 7 到图 10 所示。

图 6

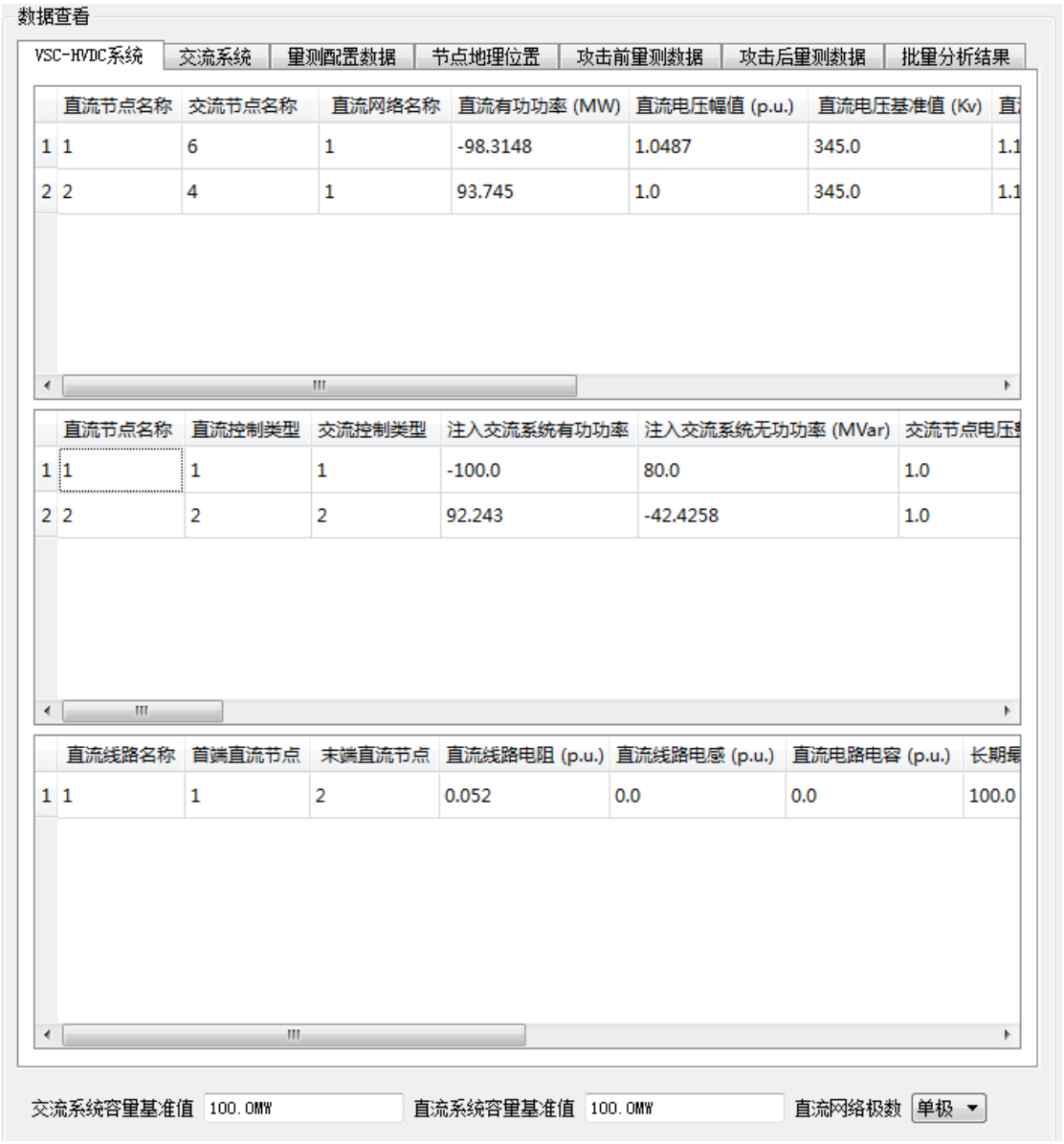
数据查看
VSC-HVDC系统
交流系统
量测配置数据
节点地理位置
攻击前量测数据
攻击后量测数据
批量分析结果
直流节点名称 交流节点名称 直流网络名称 直流有功功率 (MW) 直流电压幅值 (p.u.) 直流电压基准值 (Kv)
1 1 6 1 -98.3148 1.0487 345.0
2 2 4 1 93.745 1.0 345.0
直流节点名称 直流控制类型 交流控制类型 注入交流系统有功功率 注入交流系统无功功率 (MVar)
1 1 1 1 -100.0 80.0 1.0
2 2 2 2 92.243 -42.4258 1.0
直流线路名称 首端直流节点 末端直流节点 直流线路电阻 (p.u.) 直流线路电感 (p.u.) 直流电路电容 (p.u.)
1 1 1 2 0.052 0.0 0.0 100.0
交流系统容量基准值 100.0MW
直流系统容量基准值 100.0MW
直流网络极数 单极

图 7


数据查看
VSC-HVDC系统
交流系统
量测配置数据
节点地理位置
攻击前量测数据
攻击后量测数据
批量分析结果
交流节点名称 电压幅值量测 量测误差的标准差 注入有功量测 量测误差的标准差 注入无功量测
1 1 1 0.001 0 0.001 0
2 2 1 0.001 1 0.001 1
3 3 1 0.001 1 0.001 1
4 4 1 0.001 0 0.001 0
5 5 0 0.001 0 0.001 0
支路首端节点 支路末端节点 支路首端有功潮流量测 量测误差的标准差 支路首端无功潮流量测
1 1 2 0 0.001 0 0.001
2 1 5 1 0.001 1 0.001
3 2 3 1 0.001 1 0.001
4 2 4 0 0.001 0 0.001
5 2 5 1 0.001 1 0.001
直流节点名称 交流节点名称 注入有功潮流量测 量测误差的标准差 注入无功潮流量测 量测误差的标准差
1 1 6 1 0.001 1 0.001
2 2 4 1 0.001 1 0.001
交流系统容量基准值 100.0MW
直流系统容量基准值 100.0MW
直流网络极数 单极

图 8


数据查看
VSC-HVDC系统
交流系统
量测配置数据
节点地理位置
攻击前量测数据
攻击后量测数据
批量分析结果
交流节点名称 经度 纬度
1 1 96.2476 149.327
2 2 105.7963 130.6884
3 3 146.2866 125.7974
4 4 152.7088 148.5248
5 5 107.4019 142.9053
6 6 105.7963 156.5525
7 7 155.9199 156.5525
8 8 165.5755 163.0957
9 9 152.0562 165.2504
10 10 138.2588 162.9748
11 11 115.4297 167.7914
12 12 96.163 171.0026
直流节点名称 经度 纬度
1 1 114.2476 155.4504
2 2 145.8455 151.4504
交流系统容量基准值 100.0MW
直流系统容量基准值 100.0MW
直流网络极数 单极

图 9

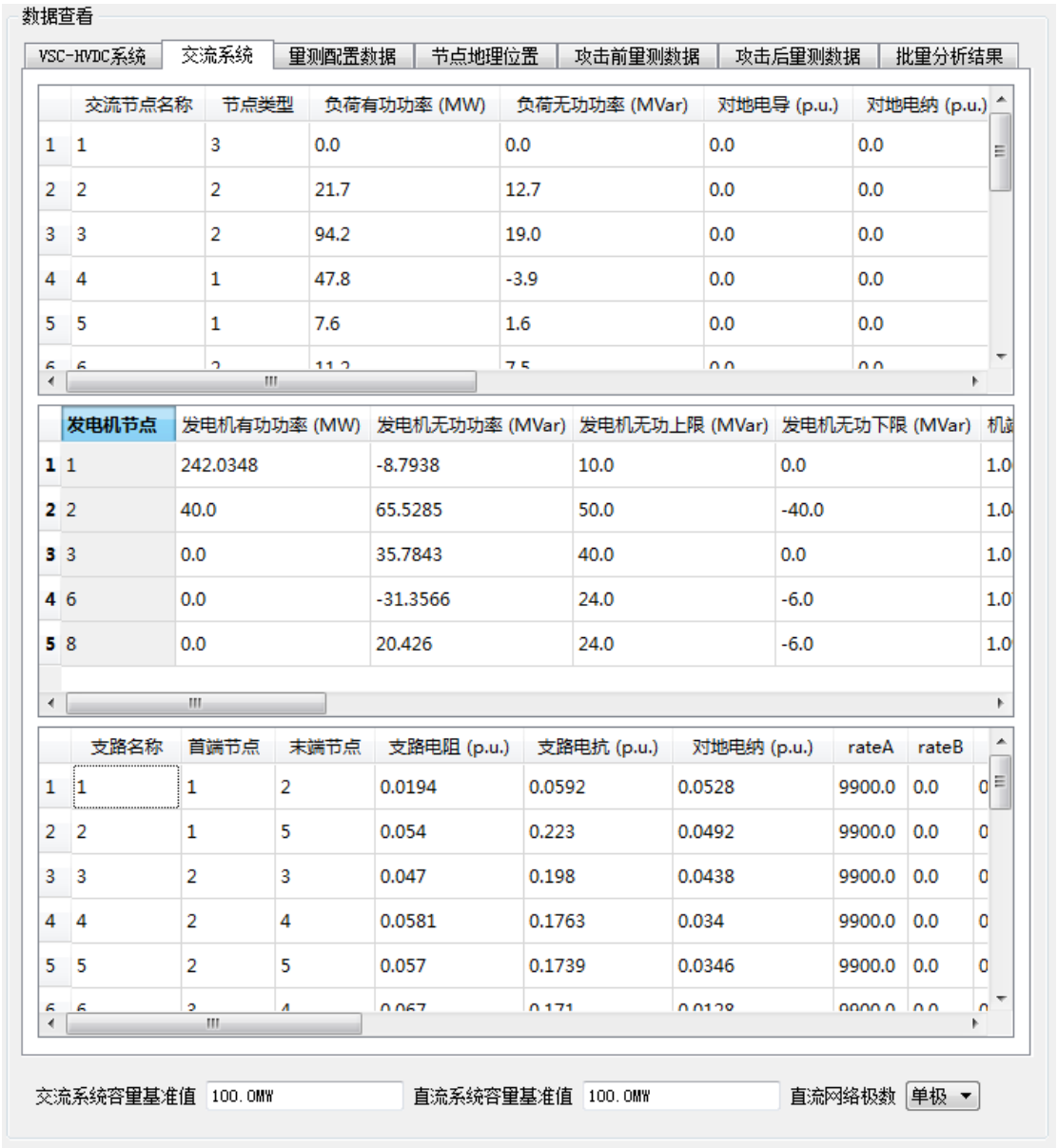

图 10

3.3 绘制单线图

点击界面中的“绘制单线图”按钮，可在界面中展示系统单线图，其中交流节点用圆圈表示，直流节点用方框表示，如图 11 所示。

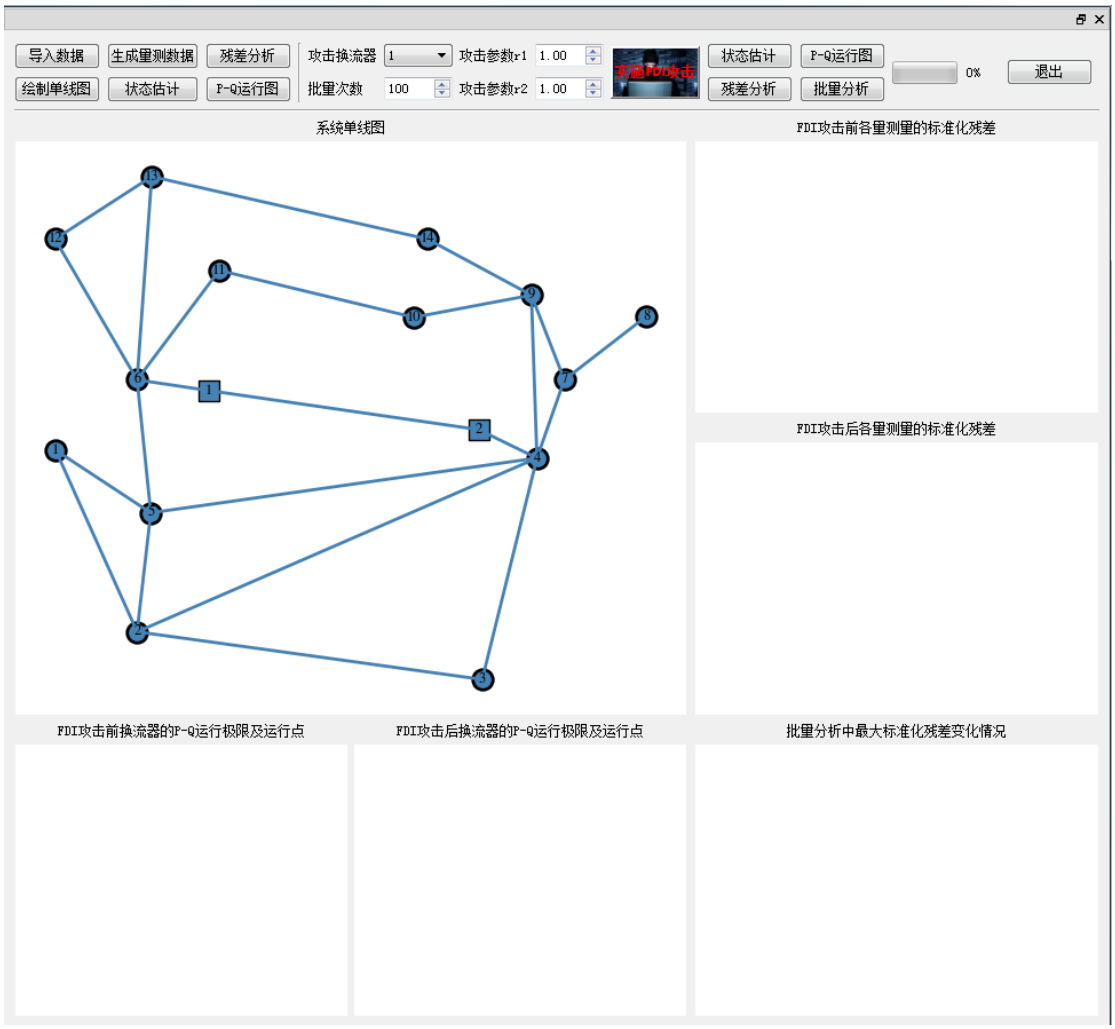

图 11

3.4 生成量测数据

点击界面中的“生成量测数据”按钮，随机生成攻击前的量测数据，并展示在数据查看部分的对应部分，如图 12 所示。

图 12

3.5 状态估计

点击界面中左侧的“状态估计”按钮，软件根据攻击前的量测数据进行状态估计计算，得到系统状态变量的估计值。

3.6 残差分析与 P-Q 运行极限分析

依次点击界面中左侧的“残差分析”和“P-Q 运行图”按钮，软件界面中得到攻击前各量测量的标准化残差和换流器的 P-Q 运行极限和运行点，如图 13 所示。

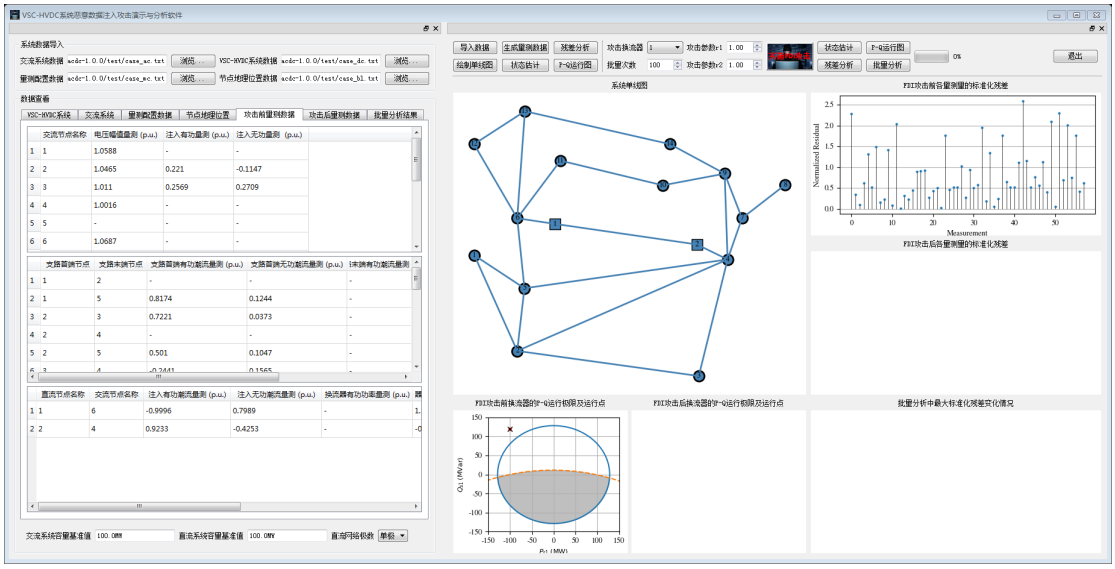

图 13

3.7 攻击参数设置

如图 14 所示，在软件中设置攻击参数，包括被攻击换流器、攻击参数 r1 和 r2 以及批量分析次数。

图 14

3.8 恶意数据注入攻击

点击界面中的“实施 FDI 攻击”按钮，被攻击换流器在单线图中用红色圆形标出，然后软件求解恶意数据注入攻击策略模型，求解完成后数据查看部分展示出攻击后的量测数据，其中被篡改的量测数据用红色标出，如图 15 所示。

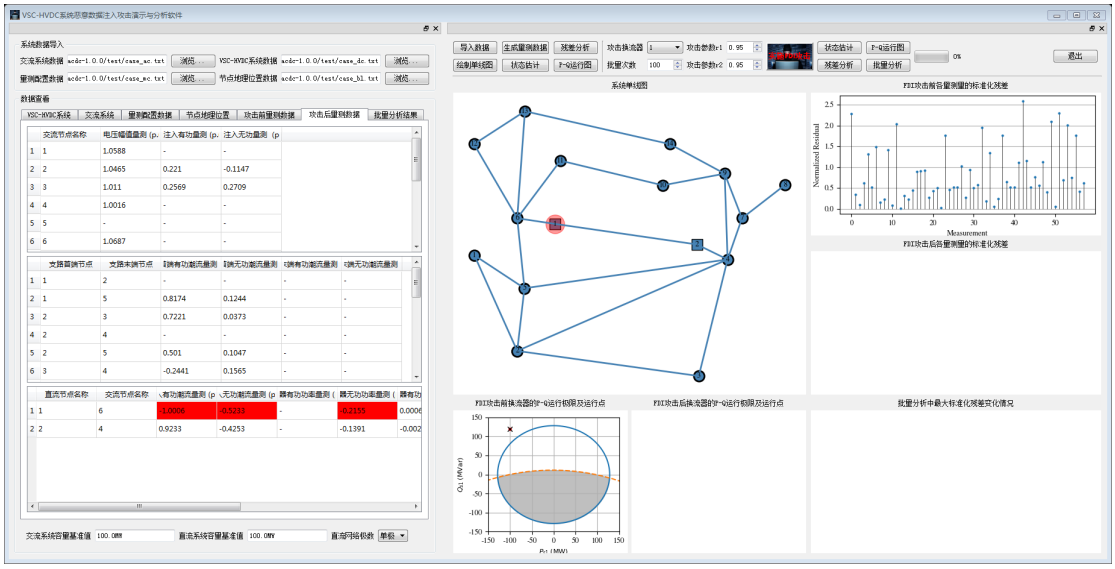

图 15

3.9 攻击后的状态估计、残差分析和 P-Q 运行极限分析

依次点击界面中右侧的“状态估计”、“残差分析”和“P-Q 运行图”，可在界面中展示攻击后的各量测量的标准化残差、P-Q 运行极限及运行点，如图 16 所示。

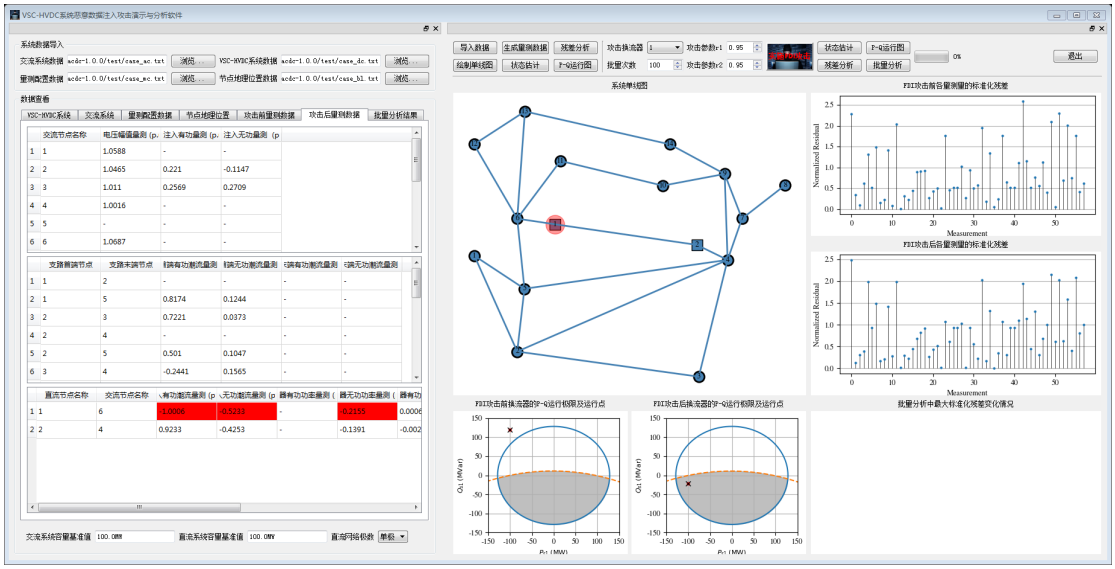

图 16

3.10 批量分析

点击界面中的“批量分析”按钮，软件执行批量分析计算，每次试验中攻击前后最大标准化残差情况分别展示为界面右下角图形和数据查看部分的表格中，如图 17 所示。另外，界面中的进度条实时反应批量分析的计算进程。

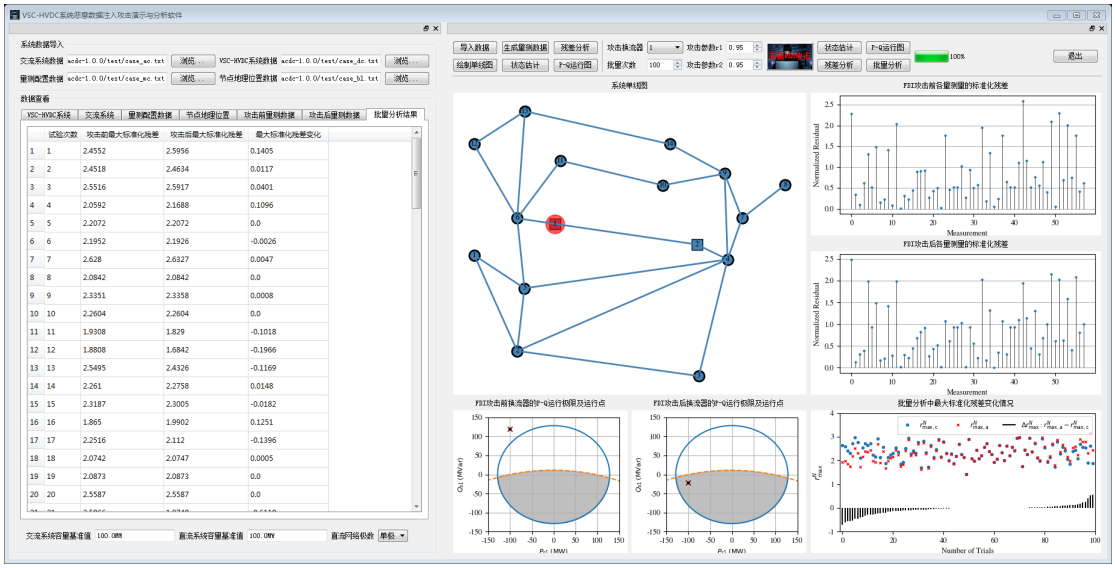
VSC-HVDC系统思维数据注入攻击演示与分析软件
系统数据导入
交流系统数据
VSC-MVDC系统数据
量测配置数据
节点地理位置数据
浏览...
数据查看
VSC-MVDC系统
交流系统
量测配置数据
节点地理位置
攻击前量测数据
攻击后量测数据
批量分析结果
试验次数
攻击前最大标准化残差
攻击后最大标准化残差
最大标准化残差变化
1 1 2.4552 2.5956 0.1405
2 2 2.4518 2.4634 0.0117
3 3 2.5516 2.5917 0.0401
4 4 2.0592 2.1688 0.1096
5 5 2.2072 2.2072 0.0
6 6 2.1952 2.1926 -0.0026
7 7 2.628 2.6327 0.0047
8 8 2.0842 2.0842 0.0
9 9 2.3351 2.3358 0.0008
10 10 2.2604 2.2604 0.0
11 11 1.9308 1.829 -0.1018
12 12 1.8808 1.6842 -0.1966
13 13 2.5495 2.4326 -0.1169
14 14 2.261 2.2758 0.0148
15 15 2.3187 2.3005 -0.0182
16 16 1.865 1.9902 0.1251
17 17 2.2516 2.112 -0.1396
18 18 2.0742 2.0742 0.0005
19 19 2.0873 2.0873 0.0
20 20 2.5587 2.5587 0.0
交流系统容量基准值 100.0MW
直流系统容量基准值 100.0MW
直流网络极数 单极
导入数据
生成量测数据
残差分析
绘制单线图
状态估计
P-Q运行图
攻击换流器
攻击参数r1 0.95
批量次数 100
攻击参数r2 0.95
批量分析
100%
退出
系统单线图
FDI攻击前各量测量的标准化残差
FDI攻击后各量测量的标准化残差
Normalized Residual
Measurement
FDI攻击前换流器的P-Q运行极限及运行点
FDI攻击后换流器的P-Q运行极限及运行点
批量分析中最大标准化残差变化情况
Number of Trials

图 17