DEVELOPMENT OF A PROBABILISTIC NATURAL GAS TRANSMISSION NETWORK SIMULATOR PROGASNET AND APPLICATIONS TO EUROPEAN NETWORKS

Vytis Kopustinskas, Pavel Praks

European Commission, DG Joint Research Centre, Institute for Energy and Transport,
E. Fermi 2749, TP230, Ispra (VA), 21027, Italy,
Email: vytis.kopustinskas@jrc.ec.europa.eu; pavel.praks@jrc.ec.europa.eu

The paper presents development of the probabilistic gas transmission network simulator ProGasNet which is aimed to address security of supply problems including network reliability, vulnerability and resilience aspects. The ProGasNet methodology combines Monte Carlo simulation technique and maximum flow algorithm from graph theory. The ProGasNet capabilities are demonstrated on a benchmark gas network of several EU countries.

I. INTRODUCTION

A number of energy supply disruptions due to economic, political or technical reasons highlight the need to study energy infrastructure networks from the security of supply point of view. After consequent gas supply disruptions during 2004-2008 period and the major supply disruption in January 2009 due to the Russia-Ukraine dispute, the European Commission (EC) reacted by issuing Regulation 994/2010 (Ref. 1) on security of gas supply, which requires the EU Member States to fulfil a number of requirements, including risk assessment, preventive action plan and emergency action plan, installation of cross border reverse flow capabilities, and supply and infrastructure standards based on the N-1 criterion. These and other measures proved to be important for the gas network resilience in a number of subsequent smaller supply disruptions (e.g. Libyan war in 2011, cold snap in early 2012).

In 2014 the EC released energy security strategy[2], highlighting strong EU dependence on imports and in particular on a few importers thus requesting the Member States to develop import diversification measures and emphasizing importance of liquefied natural gas (LNG) import terminals. In addition, the EC Connecting Europe Facility co-funds many energy infrastructure projects developed in particular to enhance security of supply in gas and electricity sectors.

Gas transmission network is part of critical infrastructure that has been recently addressed by various initiatives from research institutions and governments worldwide. The European Commission has taken the initiative to organize a network consisting of research and technology organizations within the European Union with interests and capabilities in critical infrastructure protection[3]. Interdependencies between critical infrastructures make the analysis complicated and challenging, and the topic is attracted by a growing number of researchers[4,5,6]. For energy infrastructures the most interesting interdependence is between gas and electricity networks[7].

The JRC has started to develop an in-house software tool ProGasNet for probabilistic modelling of gas transmission network with the aim to address security of supply issues including network reliability, vulnerability and other aspects.

The next section will briefly present the methodology used in the ProGasNet computational engine and the capabilities of the tool. The third section will present the gas network topology and data, followed by security of supply evaluation results to be used for gas infrastructure network risk assessment. The fifth section will present bottleneck analysis study case using ProGasNet simulator. The sixth section will present some results of vulnerability analysis and component importance analysis. The concluding remarks are given in section VII.

II. PROGASNET METHODOLOGY

From the computational point of view, the analysis of large infrastructure networks is very demanding. A detailed review[8] of the state of the art in the field of network reliability analysis presents computational complexity, exact algorithms, analytic bounds and Monte Carlo (MC) methods. The natural gas network optimization study[9] shows an example of combination of network optimal operation and physical flow computations. The Joint Research Centre (JRC) report[10] presents testing results of two approaches implemented for relatively simple benchmark network systems: Monte-Carlo (MC) reliability simulation and fault tree analysis. The results of test cases indicate potential of both methods for network reliability analysis and the need for further research. The current paper presents further development of the MC approach and provides a number of country wide or regional analysis examples.

The ProGasNet uses a distance-based approach of a stochastic network flow model. Priority based gas supply pattern is based on distances from the source node, so nodes closer to the gas source are served first. This supply pattern is typical in gas transmission pipeline networks. In each Monte-Carlo simulation step, component (pipelines, compressor stations, storages, LNG facilities) failures are sampled. Then for each network configuration consisting of failed and operational elements, maximum flow algorithm with multiple sources and multiple sinks is applied in order to estimate the maximum of transmitted flow from gas source nodes to sink nodes (gas consumers). The algorithm considers pipeline capacity and other constraints to avoid physically infeasible solutions, like different flow directions in parallel pipelines or bi-directional flow in the same pipeline (also called parasitic flow[11]). The Dijkstra's algorithm for calculating distance matrix among sources and sinks is used. Then, a permutation matrix of the graph isomorphism problem according to the distance from the gas source is computed. In this way the original model is transferred to the distance-based approach by a dynamic reordering of nodes and lines of the network graph model[12]. This graph isomorphism task is performed by linear algebra operations[13]. To finish the simulation step, the computed flow matrix is transformed back into the original problem by an inversion linear algebra operation.

Finally, Monte-Carlo simulations are used for estimating the probability of having less than demanded volume of the natural gas in each network node. The simulation approach can also be used for the bottleneck analysis, vulnerability (critical component) or component importance analysis or time-dependent storage analysis.

III. GAS NETWORK DATA AND TOPOLOGY

Figure 1 shows topology of the test case gas transmission network. It is based on a real regional network topology and data, however location is not displayed. The transmission network topology is rep-resented by a graph with nodes and links (edges). The nodes are normally the following elements:

- Demand nodes (consumers connected to the transmission network;
- Compressor stations;
- Supply nodes (storages, LNG terminals, import points at cross-borders).

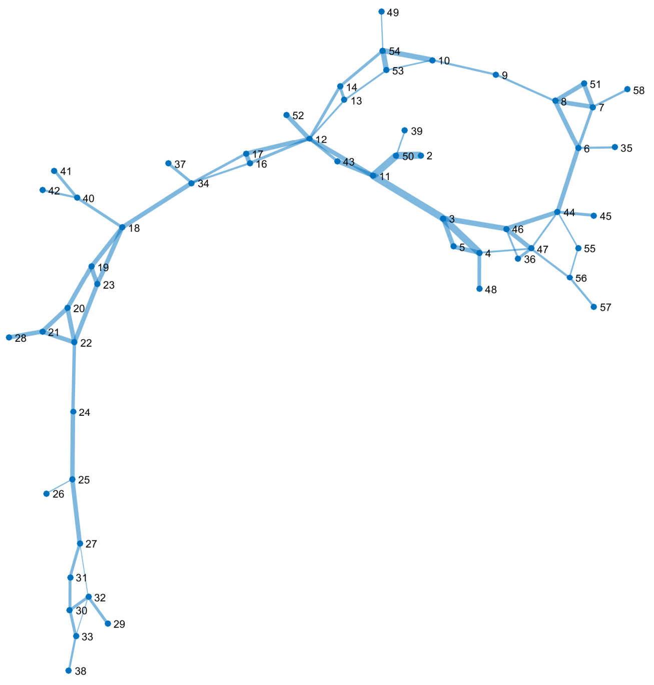

Fig. 1. Topological layout of the study network. Thickness of the edges is proportional to the pipeline capacity.

The node data entered in the model depend on the node type. The demand nodes require only daily demand value (Table I). This value is normally peak demand value, but it could be also average winter or summer consumption value depending on the purpose of the model.

TABLE I. Network demand nodes, in millions of cubic meters per day (mcm/d).

Node	Demand	Node	Demand
4	0.1	34	0.5
5	3.2	35	0.1
6	0.1	36	4.2
7	0.3	37	1.3
9	0.1	39	0.3
10	1	41	0.6
13	0.5	42	0.6
17	0.1	43	0.2
18	8.5	44	0.7
20	0.6	45	1.3
25	0.5	47	0.5
26	0.8	48	1.8
27	3	49	0.2
28	6	51	7
30	0.5	52	0.6
33	0.5	53	0.1

Table II shows maximum capacities and type (pipeline, UGS or LNG) of input supply nodes. In case of underground gas storages (UGS), also the output values of not fully loaded storages can be used.

Table II. Maximum supply capacity.

Node	Type	Capacity, mcm/day
2	Pipeline	31
11	Pipeline	7
19	UGS	30
4	Pipeline	4
10	LNG	10.2

The total maximum supply capacity is 82.2 mcm/d. The total network peak demand is 45.8 mcm/d, therefore the network has certain degree of spare capacity to compensate supply disruptions. All pipeline sections including their estimated capacity and lengths are available in the model, but not shown due to space limitations. For each network component, failure data must be provided. The following components (nodes) are considered for failures with corresponding failure frequencies:

- Compressor station (CS) failure: 2.5E-01/yr;
- Underground storage failure: 1.0E-01/yr
- LNG terminal failure: 1.5E-01/yr
- Pipeline failure: 3.5E-05 /km/yr.

The model considers one month interval for computations. It is assumed that the same peak consumption in the network is constant during this one month period.

The CS failure rate was computed using a typical model of a CS station and industrial reliability data. The UGS failure estimate is an expert estimate. The LNG failure estimate is based on literature references[14]. The pipeline failure rate was taken from pipeline incident database[15] and assuming that rupture occurs 10 less frequently as incident.

The compressor station node is modelled as working or failed (on/off), for each state determining the corresponding capacity of the outgoing pipelines. The capacity reduction due to compressor station failure is normally estimated by hydraulic model computations or expert evaluation. As a consequence due to a CS failure, capacity reduction by 20% of the inlet pipelines and also the outlet pipelines until the next connection node is assumed. This assumption is based on physical flow models, however is not accurate in all cases and also multiple CS failures will have more severe effects on the network operation. Currently physical model is being developed in order to estimate the effect of the CS failures more precisely.

IV. SECURITY OF SUPPLY EVALUATION

The pipeline import sources are not considered to fail due to lack of upstream network model, however they are modelled as on/off elements by scenario analysis. The following main 4 supply scenarios were analysed:

- Scenario A: All currently available sources. Scenario A represents basic scenario when all sources can be used for supply.
- Scenario B: All curently available sources, except Node 10. Scenario B runs the model with Node 10 (LNG) unavailable. This scenario provides an indication of the importance of the terminal for security of supply to the region. Such scenario can happen due to technical failure of the facility or connecting pipelines ir failure to deliver LNG by sea.
- Scenario C: All curently available sources, except Node 2 supply. Scenario C models situation when supply from Node 2 is unavailable. This scenario can test the system when the largest supply source is unavailable.

Scenario D: All curently available sources, except Node 19. Scenario D assumes that Node 19 (UGS) is unavailable due to technical problems, failures or inability to fill it up during summer period. This scenario is used to demonstrate importance of the storage to the whole network.

The results also display scenarios E/F/G/H which equivalent to scenarios A/B/C/D respectively, but with Node 11 unavailable. This can be used to test importance of the source node 11.

The probabilistic model is run for 1 million times and collects statistical estimates of various parameters in the network. The same results can be presented in different ways: statistical tables, probability tables or cumulative distribution function (CDF) plot. All three types of results are derived from the same sample and represent the same results, but highlights different points of view of the results. The probabilistic and statistical results are computed for a period of one month. For this time period, peak demand is considered to be stable and represent a critical period of severe winter. This assumption is considered to be conservative. Regarding the component failures, no repairs are considered. All failures are considered to occur during a period of one month, although they do not occur at the same moment. This is again a conservative assumption, but as our focus is security of supply, conservative assumptions are widely accepted in the probabilistic studies.

Table III presents probabilistic results for the whole network demand and all scenarios. The network is well supplied in scenarios A/B/E and F, however scenarios D/H and C show obvious vulnerabilities in the network. The results indicate that supply in the region is not homogenous, but fragmented into two areas. The first area is strongly dependent on Node 2 supply source and the second – on Node 19 source. This is very evident because scenario C affects only one area and scenario D affects only the other area. These results are very evident when analysing not the total network supply, but area supply under given scenario. The probabilistic results are available for each scenario, but in the post-processing phase the CDFs are compared by Kolmogorov-Smirnov test and those that are statistically similar are displayed together, meaning that there are no statistically significant differences among them, e.g. scenarios A/B/E/F in Fig. 2. All scenarios supply at least 50% of the demanded gas by the network with acceptable security of supply: probability of having less than 50% of needed gas is in the range of 8E-03 – 2E-06 per month.

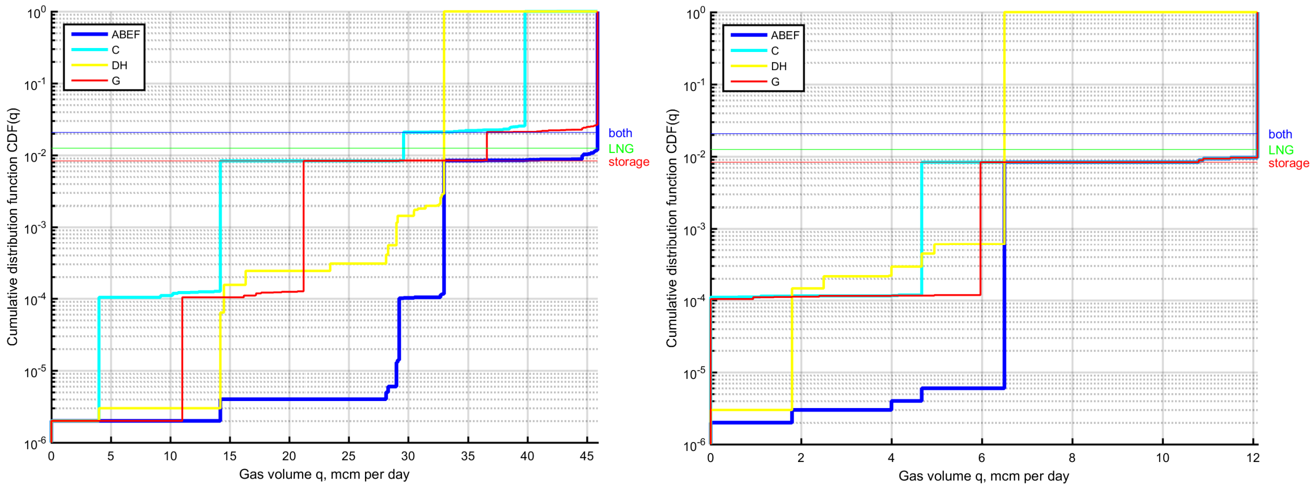

Fig. 2. CDF plots for the total network demand of 45.8 mcm/d (left) and one part of the network (demand 12 mcm/d).

TABLE III. Probabilistic results for the whole network supply for all scenarios (D=45.8 mcm/d). D – demand volume, Mean – average available gas volume.

Scenario	D-Mean	P(X=0)	P(X<0.2D)	P(X<0.5D)	P(X<0.8D)	P(X<D)
DH	12.9	0	1.0E-06	2.4E-04	1	1
C	6.5	0	1.1E-04	8.3E-03	2.2E-02	1
G	0.3	0	0	8.3E-03	2.1E-02	2.7E-02
ABEF	0.1	0	0	2.0E-06	8.5E-03	1.2E-02

The same results can be explored graphically by CDF plots (Fig. 2). The plot shows that scenarios D, H and C cannot supply all the needed gas and indicates the available maximum volume of gas. The scenarios A, B, E, F and G can supply all the needed gas, but with different reliability levels. Such results are available for each network node or specified area (e.g. one country), but due to space limitations only two CDF plots are shown.

V. BOTTLENECK ANALYSIS STUDY CASE

As ProGasNet algorithm computes flows in each network link, bottleneck analysis is a quite straight-forward task. A criteria for a potential bottleneck is pipeline free capacity factor (PFCF) – percentage ratio of the difference between maximum capacity and average flow in the pipeline segment to its maximum capacity (Eq. 1). The ProGasNet was adjusted to make these calculations for each scenario by aggregating parallel pipelines.

$$PFCF = \frac{Maximum\ Capacity - Average\ Flow}{Maximum\ Capacity} \times 100\% \qquad (1)$$

As a result, no bottlenecks were identified in the scenarios A, B, E and F, as all pipelines had rather high PFCF. However, in scenarios C, D, G and H a number of bottlenecks were identified. The results were filtered not to display source nodes and small pipelines to end users which are sometimes flagged as potential bottlenecks although they are not connecting any other network node. Below, an iterative bottleneck identification process will be described for scenario D:

- Step 1: Pipeline 17->34 (capacity 6.5 mcm/d) has PFCF=0%. Capacity is increased from 6.5 to 15 mcm/d;
- Step 2: Pipeline 34->18 (capacity 12.1 mcm/d) has PFCF=0.6%. Capacity is increased from 12.1 to 15 mcm/d;
- Step 3: Pipeline 17->34 (capacity 15 mcm/d) has PFCF=0.7%. Capacity is increased from 15 to 18 mcm/d;
- Step 4: Pipeline 34->18 (capacity 15 mcm/d) has PFCF=1.3%. Capacity is increased from 15 to 18 mcm/d;
- Step5: Pipeline 10->9->8 (capacity 2.8 mcm/d) has PFCF=1.2%. Capacity is increased from 2.8 to 5 mcm/d;
- Step 6: Pipeline 10->9->8 (capacity 5 mcm/d) has PFCF=1.4%. Capacity is increased from 5 to 8 mcm/d;
- Step 7: The calculations used values the previous step. No more potential bottlenecks were identified.

As clear from the above steps, some pipelines appear as bottlenecks several times after virtual increase of other pipelines capacity. Steps 5 and 6 indicate that selection of a new virtual capacity is a problem and might require several trials. Figure 3 shows the effect of Steps 1-2-4-7 to the whole network and the same network area as in Fig.2. The whole network benefits from all the process steps 1-7, however for the selected network area there is no statistically significant difference among the steps 2-7: the supply situation cannot be longer improved in that part of the network. Similarly, the results can be analysed for all the demand nodes and areas.

The bottleneck analysis iterative process for scenario C runs as follows:

- Step 1: Pipeline 34->17 (capacity 6.2 mcm/d) has PFCF=0.9%. Capacity is increased from 6.2 to 12 mcm/d;
- Step 2: Pipeline 18->34 (capacity 12.1 mcm/d) has PFCF=1.3%. Capacity is increased from 12.1 to 15 mcm/d;
- Step 3: Pipeline 34->17 (capacity 12 mcm/d) has PFCF=0.9%. Capacity is increased from 12 to 15 mcm/d;
- Step 4: The calculations used values the previous step. No more potential bottlenecks were identified.

Interestingly, bottleneck analysis for scenarios C and D identifies the pipelines 18-34-17 as major bi=directional bottlenecks in the network. This finding confirms the conclusion that the network is not homogenous and supply nodes 2 and 19 supply two different parts of the network with a bottleneck connection between them. Note that under normal operation condition of the network, no bottlenecks were identified and they appear only when major supply nodes are unavailable.

Scenarios G and H identify almost identical connections as bottlenecks, connection 18-34-17 being the most significant. This suggests that planned new connection in Node 11 might not be fully utilised by the network consumers due to existing bottlenecks in the system.

The other identified congested segments are limited by the source supply capacity which is outside the control of the system operator and require either expensive supply infrastructure development solutions or international agreements.

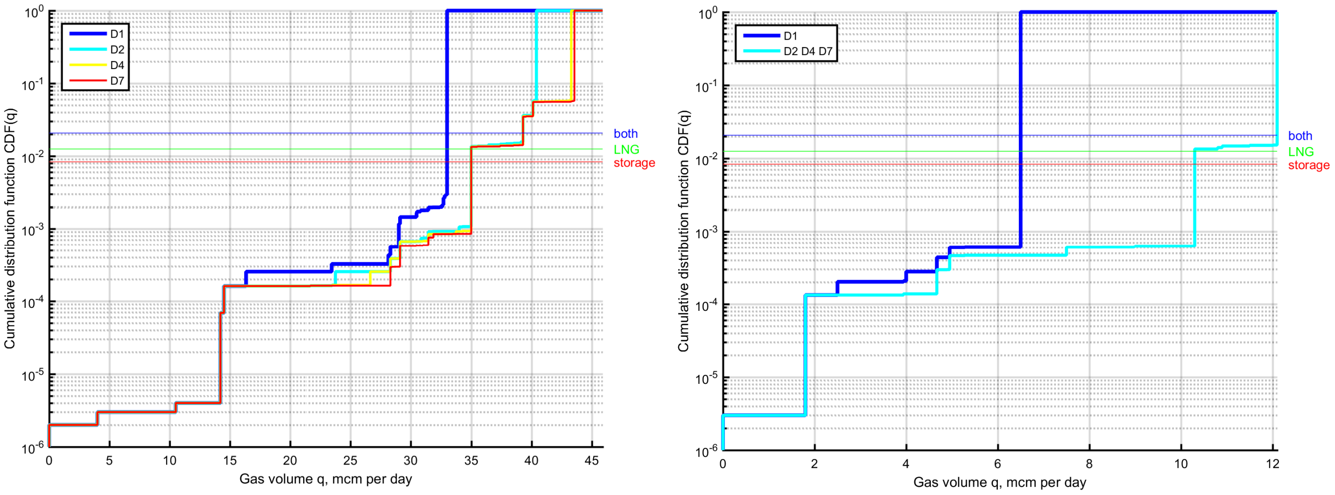

Fig.3. CDF plots showing effect of the bottleneck steps 1-2-4-7 for the total network demand of 45.8 mcm/d (left) and one part of the network (demand 12 mcm/d).

VI. VULNERABILITY AND COMPONENT IMPORTANCE ANALYSIS

Vulnerability analysis can be considered in a number of perspectives[16]. The Monte Carlo model used for reliability analysis can be successfully employed for vulnerability analysis, however certain analysis patterns change. From global vulnerability analysis perspective, the model can be run not with randomly failing network components, but by enforcing failures of the components or increasing consumption demand in deterministic manner. The results of such an analysis are outside the scope of this paper, but such a study can be performed with little programming efforts of the existing ProGasNet code. From critical component analysis perspective, the largest negative consequences are determined under failures of each component or their groups. Having already performed reliability analysis and as a bunch of simulations and their results are available, a ProGasNet software module has been developed to extract the most critical components in terms of the largest negative consequences.

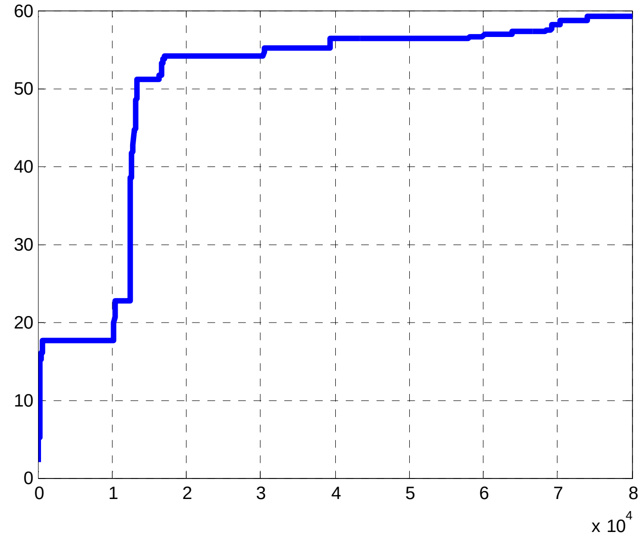

Fig. 4. Vulnerability analysis: Index of Monte-Carlo simulation step versus the sorted total available gas supply of 80 000 simulations (out of 1000000).

Firstly, the sum of supply from all Monte-Carlo simulations is sorted over all nodes by the ascending order. Results of the first 80 000 values are presented in Figure 4. These results include both the theoretical minimum supply and also the maximum theoretical supply, so it is not necessary to analyse a larger set of simulations.

It is possible to zoom into each step of Figure 4 and extract which component failure has caused it and what are the consequences (how much gas is available in the network). The analyst can be especially interested in long horizontal lines of the plot in Figure 4, as these cases are more likely than those with short horizontal lines. However, at the end a trade-off between likelihood and severity of consequences should be considered.

Table IV shows as an example detailed results of vulnerability analysis for selected supply levels for 2 country network[17]. For the each supply level, the total available gas supply, failure sequence, and its likelihood expressed by the frequency are presented. According to Table IV, the supply level 4 implies a reduction of the available supply to 17.7 mln m^3/d. Detailed analyses of Monte-Carlo results showed that this supply level is caused by a single pipeline failure between nodes 2 and 3. The vulnerability analysis showed that the analyzed network includes a variety of failure combinations, which can significantly reduce the total supply. The software tool ProGasNet is able to analyze all these cases.

However, in this section of the paper only brief demonstration is given to show the potential of the ProGasNet vulnerability module.

TABLE IV. Detailed results of vulnerability analysis for selected supply levels.

Supply level	Total available gas supply, mln m^3/d	Failure sequence	Estimated frequency of failure sequence
1	2	Pipelines:(2,3), (8,9) Nodes:17	5.00E-06
2	2.7	Pipelines:(2,3) Nodes:10, 17	2.00E-06
3	5.2	Pipelines:(2,3) Nodes:17 (99.1% of cases)	2.32E-04
		Pipelines:(3,4),(3,5) Nodes:17 (0.9% cases)	
4	17.7	Pipelines:(2,3) Nodes: -	1.02E-02

The ProGasNet simulator also includes another module to identify important components in the network[18]. The approach is based on computing Risk Achievement (RA) value (Eq. 2) for all network components and disruption scenarios A-H as described in Section IV.

$$RA = R(x_j=1) - R(base) \qquad (2)$$

Results of 1 million of Monte-Carlo simulations applied to the network as described in Section III clearly shows that components of the network back-bone can be grouped on the three different importance groups. For example, disruption scenarios from the most important first group leads to fatal loss of supply consequences on the given risk level with risk achievement value ~0.99. Fortunately, majority of failure consequences of the largest gas source (Node 2) can be reliably compensated by the LNG terminal (Node 10). Although the gas network uses redundant gas sources, simulated results clearly show that the gas network is very sensitive to disruptions leading to disconnection (or a failure) of the second largest gas source storage (Node 19).

VII. CONCLUSIONS AND DISCUSSION

The paper describes the methodology approach and some results obtained by the probabilistic gas network simulator ProGasNet software tool. The ProGasNet has been applied to gas transmission networks of several EU countries, however geographical information cannot be disclosed. Various types of analysis have been performed: reliability, vulnerability, security of supply and various types of results have been reported: supply reliability estimates, security of supply under different disruption scenarios.

The ProGasNet model provides an indication of the worst networks nodes in terms of security of supply and provides their numerical ranking. It is recommended to use the results of the model in a qualitative (comparative) way rather than interpret numerical values directly. The model is very powerful to compare and evaluate different supply options, new network development plans and analyse potential crisis situations.

The model has a number of advantages and limitations that must be considered by interpreting the results. The model at this stage cannot model adequately consequences of failures of compressor stations. Currently, it is assumed that pipeline capacity is reduced by 20% in the nearest connections, however this assumption needs to be validated by physical flow computations. Failures of two nearby compressor stations would have severe effect on the network capacity, but this event is not considered in the current version of the probabilistic model. Further work is needed to overcome these limitations.

The results indicate that supply in the analyzed network (Section III) is not homogenous, but fragmented into two areas. The first area is strongly dependent on Node 2 supply source and the second – on Node 19 source. This is very evident because ‘Node 2 unavailable’ scenario C affects only one area and ‘Node 19 unavailable’ scenario D affects only the other area.

The bottleneck analysis was performed in interactive steps and the major bottleneck was identified between two regions in the network. The bottleneck detection methodology first virtually eliminates the most significant bottleneck and then reruns the model. The next step identifies more bottlenecks although they were not detected in the first step. This process finally provide very evident result: connection 17-34-18 is a bidirectional bottleneck in the network when either source is lost in one or another side of the network. The other identified congested segments are limited by the source supply capacity which is normally outside the control of the system operator and requires either expensive supply infrastructure development solutions or international agreements.

The ProGasNet approach was used also to perform vulnerability analysis and component importance ranking. These are rather recent developments of the simulator and are shown only with the purpose to demonstrate capabilities of the tool.

Despite the limitations of the simulator, essentially caused by lack of pressure parameter in the computational engine, the results of the networks studied by ProGasNet provide realistic findings that are recognized by the system operators.

REFERENCES

1. Regulation (EU) No.994/2010 of the European Parliament and of the Council of 20 October 2010 concerning measures to safeguard security of gas supply and repealing Council Directive 2004/67/EC. Official Journal of the European Union, 2010.
2. European Energy Security Strategy, Communication from the Commission to the European Parliament and the Council, Brussels, Belgium (2014).
3. A.M. LEWIS, D.WARD, L.CYRA and N. KOURTI, "European Reference Network for Critical Infrastructure Protection", *Int. J. Crit. Infrastruct. Protect.* **6**, 51-60 (2013).
4. R. SETOLA, S. DE PORCELLINIS and M. SFORNA, "Critical infrastructure dependency assessment using the input–output inoperability model*", Int. J. Crit. Infrastruct. Protection*, **2**, 170-178 (2009).
5. M. OUYANG, "Review on modeling and simulation of interdependent critical infrastructure systems", *Reliab. Eng. Syst. Safety*. **121**, 43-60(2014).
6. P. TRUCCO, E. CAGNO and M. DE AMBROGGI, "Dynamic functional modelling of vulnerability and interoperability of Critical Infrastructures*", Reliab. Eng. Syst. Safety*, **105**, 51-63 (2012).
7. B. CAKIR ERDENER, K. A. PAMBOUR, R. BOLADO LAVIN and B. DENGIZ, "An integrated simulation model for analysing electricity and gas systems", *Electrical Power and Energy Systems*, **61**. 410-420 (2014).
8. M. O. BALL, C.J. COLBOURN and J.S. PROVAN, Network Reliability, University of Maryland, USA (1992).
9. F. RØMO, A. TOMASGARD, L. HELLEMO and M. FODSTAD, "Optimizing the Norwegian natural gas production and transport", *Interfaces*, **39**(1), 46–56 (2009).
10. V. KOPUSTINSKAS and P. PRAKS, "Development of gas network reliability model", JRC technical report JRC78151, European Commission, Luxembourg (2012).
11. M. TODINOV, "Parasitic flow loops in networks", *International Journal of Operations Research*, **10(3)**, 109-122 (2013).
12. N. DEO, "Graph Theory with Applications to Engineering with Computer Science", Prentice Hall, USA (2008).
13. M.S. BAZARAA, J.J. JARVIS, and H.D. SHERALI, "Linear Programming and Network Flows", John Wiley & Sons, New York, USA (2010).
14. M. J. JUNG, J.H. CHO and W. RYU, "LNG terminal design feedback from operator's practical improvements", *The 22nd World Gas Congress proceedings*, Tokyo, Japan (2003).
15. *8th Report of the European Gas Pipeline Incident Data Group EGIG*. Groningen, Netherlands (2011).
16. J. JOHANSSON, H. HASSEL and E. ZIO, "Reliability and vulnerability analyses of critical infrastructures: comparing two approaches in the context of power systems", *Reliab. Eng. Syst. Safety*, **120**, 27-38 (2013).
17. V.KOPUSTINSKAS, P.PRAKS, "Probabilistic gas transmission network simulator and application to the EU gas transmission system", *Journal of Polish Safety and Reliability Association*, *Summer Safety and Reliability Seminars*, **6**(3), 71-78 (2015).
18. P.PRAKS, V.KOPUSTINSKAS, "Identification and ranking of important elements in a gas transmission network by using ProGasNet", Proceedings of ESREL'2016 conference, September 25-29, Glasgow, UK (2016).