Interpretation And Gas Distribution Net Threat Attack Markov models

Oleg Syrovatsky[1,2*]

[1] LLC "Gazprom mezhregiongaz engineering"
[2] National Technology Initiative Center for Advanced Manufacturing Technologies based on the Institute of Advanced Manufacturing Technologies of Peter the Great St. Petersburg Polytechnic University Polytechnicheskaya, 29, St.Petersburg, 195251, Russia

Abstract. This paper will focus on mathematical models to reduce the possibility of gas distribution net threat attacks, in order to avoid environmental damage caused by the siphoning off gas. These models are based on Markov models and theory of graphs. The article also shows some forms of attacks on gas distribution net. Environmental damage includes thermal influence caused by gas inflammation, terrain disturbance, biochemical processes. Among siphoning off gas indicators are: Interference in gas meter; Documentation noncompliance; Gas distribution off-the-meter; Power counter range discrepancy; Gas meter failure; Expired recalibration interval; Gas siphoning; Other discrepancies.

Keywords: environmental damage, siphoning off gas, Markov Model

1 Introduction

According to the experience, an unauthorized tampering into gas distribution net has a highly negative influence on our environment. The siphoning off gas leads to corrosion, gas explosion and fires, excess gas flow rate, lack of funds for environmental remediation.

The main gas pipeline failure statistical analysis has showed the following: among all pipeline failures on trials and during operation, about 10% failures caused a significant environmental damage. Herewith the big diameter pipelines 1000-1400mm are of the highest ecological hazards. Average annual gas loss which leads to the environmental pollution is 43,2 million m³. The distinctive feature of pipeline anthropogenic impact on the environment is a thermal influence caused by gas inflammation and terrain disturbance as well. The range of thermal influence that defines the area of total terrain disturbance is from 30 to 600 m, and the pit that appears during pipeline accident has maximum dimensions until 106*56*12 m. The anthropogenic impact on the environment is multiple, because it influences the biochemical processes of atmosphere, earth and water. So, the environmental pollution is caused by gas flaring, compressor stations operation, emergency emissions and others. [1].

* Corresponding author: sov708@yandex.ru

In order to avoid environmental damage it is important to reduce the possibility of siphoning off gas, so, that is why we have developed the gas distribution net threat attack model in this research.

2 Materials and Methods

Threat Attack Markov Model as systems of failures and recoveries. Siphoning gas leads up to both expected funds loss and a dangerous violation, which may cause severe accidents including fatality. In fact, to avoid threat of gas siphoning it is necessary to reduce vulnerabilities of gas distribution net. If we define the possibility of safety system to be ready for operation as Pse, then the possibility of gas siphoning threat protected gas distribution net to be ready for operation without siphoning off gas,P0se using this kind of safety system which completely reduces the vulnerability threat, can be defined as following:

$$P0se = 1 - (1 - P0y)(1 - Pse), \quad (1)$$

whereP0y – the possibility of vulnerability threat protected gas distribution net is ready to operate without siphoning off gas;

P0y – the possibility of avoiding siphoning off gas;

Pse – the possibility of gas distribution net is ready for operation.

As there are several vulnerabilities in gas distribution net, then we will have the following equation 1:

$P0se = 1 - (1 - P0y) \prod_{i=1}^{n} (1 - Psei)$

It is important to point out that this model is correct in case the elements of safety system, vulnerability and threat are independent. Which means if one of the siphoning gas threats increases other vulnerabilities of the system then it is necessary to build up the matrix of dependent vulnerabilities and threats. That is the safety system is aimed both on reducing the possibility of specific threat and on providing the independency of safety system from siphoning gas threats.

We will consider gas distribution net regarding to both arising and reducing of siphoning gas vulnerability threat and arising and reducing threat attack in general appearing by corresponding combination of vulnerability threats, as a system of failures and recoveries.

Let us build up the Markov model describing the process of arising and reducing the real threat of siphoning gas. Having this goal, we will review a mathematic description of Markov process with discrete state and continuous time taking the example of siphoning gas threat graph having two node-weighted vulnerabilities: the threat is caused by two vulnerability threats with corresponding parameters – the intensity of recoveries and the removal of vulnerabilities. We suppose that both vulnerability threats match the condition $\rho\rho \leq 0{,}2$. The probability process state system graph (Markov process) is shown in Fig.1. The graph shows four possible states of system: $S0$ – initial state of system, $S1$ – the first vulnerability in system is defined and not solved, $S2$ – the second vulnerability in system is defined and not solved, $S12$ – both vulnerabilities in system are defined and not solved – a real threat of siphoning gas is created. It is obvious to suggest that all transitions from one state to another happen under influence of simplest events with corresponding intensity of recoveries and removal of vulnerabilities.

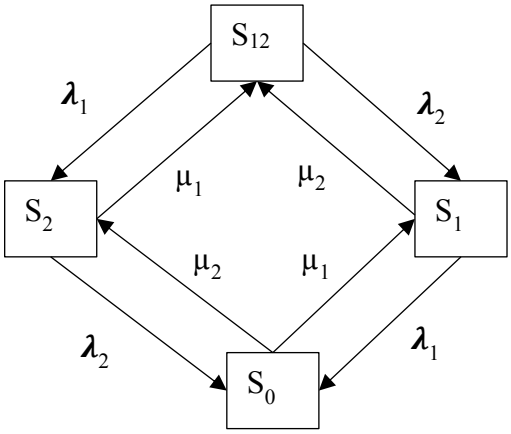

Fig.1. Markov model describing the process of arising and reducing the real threat of siphoning gas

Kolmogorov differential system for state probabilities of this graph will be as following:

$$P_0^{/} = \mu_1 P_1 + \mu_2 P_2 - (\lambda_1 + \lambda_2) P_0$$
$$P_1^{/} = \lambda_1 P_0 + \mu_2 P_3 - (\lambda_2 + \mu_1) P_1$$
$$P_2^{/} = \lambda_2 P_0 + \mu_1 P_3 - (\lambda_1 + \mu_2) P_2$$
$$P_{12}^{/} = \lambda_2 P_1 + \lambda_1 P_2 - (\mu_1 + \mu_2) P_{12}$$

When replacing in Kolmogorov equations their derivatives with zero values, we will get a system of linear algebraic equation, describing a steady mode, calculating which, considering exhaustive events, that means using a condition:

$$P0 + P1 + P2 + P12 = 1,$$

we will find required extremum (final) state probabilities.

Applying to our simulation task, a state S12 is of highest interest – both vulnerabilities are revealed in system, characterized by the possibility $P12$ – this is a state, where it is possible to siphon off gas (a severe threat arises), because we revealed but didn't solve all vulnerabilities that are necessary to siphon off gas. So, we can take this parameter as a possibility of siphoning gas (Pya= $P12$). Consequently, the probability of system operational readiness regarding the siphoning gas threat $PP0$a (or steady state availability Kf) is defined as:

$$Kf = P0a = P0 + P1 + P2$$

3. Extended Threat Attack Markov Model as systems of failures and recoveries of safety performance.

The extended threat attack model is important to calculate the following key parameters of threat attack: arising intensity $\boldsymbol{\lambda}$a and reducing intensity μa of the real threat attack, and failure mean operating time (recoverable system) of safety performance $\boldsymbol{T0}$y, which defines an average interval between safety performance failures – a severe threat attack arising periods. The basis of extended modelling is the usage of assessed failure rate.

In Markov reliability models the assessed failure rate ω is defined (for steady state area) as:

$$\boldsymbol{\omega = \sum i \in Q1\ Pi \sum j \in Q2 - \lambda ij,}$$

where $\boldsymbol{Q}1$ – is a set of states of system availability, $\boldsymbol{Q}2$ – a set of states of system failure, $\boldsymbol{\lambda i}$j – transition intensity from $\boldsymbol{i}$ – state of operability, probability of system $\boldsymbol{Pi}$, to j – state of nonoperability.

Assessed failure rate, characterizing the frequency of failures in recoverable systems is inversely proportional to the mean time between failures Tm, MTBF (Mean Time Between Failures), strong evidence of this relation is shown in renewal theory: $T\text{m} = 1/\omega = T0\text{y} + T\text{b}$, where $T_\text{в}$ – mean recovery time. Assuming that $\text{Kf} = T0\text{y}\ T0\text{y} + T\text{b}$, we have $T0\text{y} = \text{Kf}/\omega$. In order to build the extended threat attack model we have to get back to the graph in Fig.1 to find out the way the flow of failures of safety performance appears and to find the way to define its efficiency. As we can see the threat attack is being created in two cases: in transition of state $SS1$, where the system is with probability $P1$ (in Markov model the state probability is interpreted as a relative time share of system being in this state) , into state $S12$ (this is a severe threat attack state) the transitions happen with intensity $\lambda 2$ (if we take into account the corresponding time share of system being in state $S1$,then the intensity will be $P1\ \lambda 2$), and in transition of state $S2$, where the system is with probability $P2$, into state $S12$ the transitions happen with intensity $\lambda 1$(if we take into account the corresponding time share of system being in state $S2$, then the intensity will be $P2\ \lambda 1$). In our case the flow of failures can be interpreted as the flow of severe threat attack with intensity λa:

$\lambda\text{a} = \omega = P1\ \lambda 2 + P2\ \lambda 1$

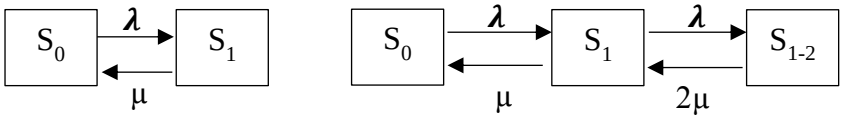

Fig.2. Stationary process state systems graphs for threat attacks

The extended threat attack model is described by graph of Fig.2, where in a specific way λa and μa are defined the intensities of transitions, $S0$ state corresponds to reducing the threat, and $SS1$ – to arising of severe threat attack. Other desirable parameters of threat attack are calculated as follows: $T0\text{ya} = 1/\lambda\text{a}$ $\mu\text{a} = \lambda\text{a}$ $\text{Kf}\ 1 - \text{Kf} = 1/T_\text{в}$

Analyzed Markov models can be used in general safety properties assessment of specific safety equipment. When modeling the gas distribution protection facilities and evaluating safety level, it is important to take into account the readiness of an intruder for a severe threat attack. This is mostly caused by the judgmental factor that define the motivation of the intruder of siphoning gas. This is the vital difference of gas distribution net modeling from the same kind of modeling in reliability theory.

4. Results

The practical outcome of siphoning off gas.

The table below illustrates the statistical analysis results of gas siphoning.

Table 1. Gas siphoning statistical analysis results

Indicators	North Ossetia Alania	Ingushetia
Interference in gas meter	522	311
Documentation noncompliance	93	1595
Gas distribution off-the-meter	14	17
Power counter range discrepancy	206	192
Gas meter failure	111	59
Expired recalibration interval	154	112
Gas siphoning	127	259
Other discrepancies	75	311

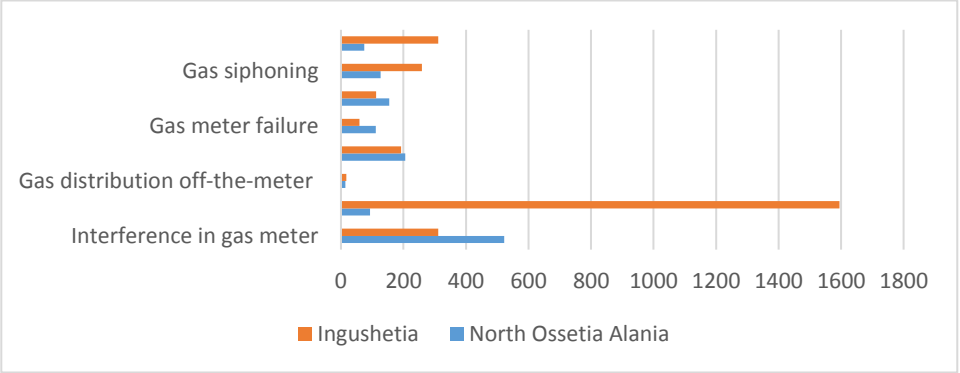

Fig.3. Gas siphoning statistical analysis results

We suggest the method of estimated gas rate loss.

1. We define gas rate according to the gas piping diameter Q_n , m³\h:

$$Q_n = 3600 * \mu * S_o * W_{gas}$$

where μ – orifice coefficient,

S_o – orifice area in gas pipe line or technical device for gas extraction,

W_{gas} – gas velocity, when it goes out of orifice to the atmosphere, m/s

2. We set the calculation period (24-hour period) when the gas was siphoning off 24 hours a day and then we calculate the gas volume, which was consumed during this period.

As follows:

$$V_n = Q_n * 24 * \text{n}$$

where 24 is the number of hours a day,

n – calculation period, a day.

The calculation was carried out according to recommendations of Legal Office of "Gazprom mezhregiongaz". The calculation matches the calculation method of Order №975 of the Ministry of Energy of the Russian Federation, but without direct reference.

The gas rate loss of one of the objects was 176 076 m³ assuming 6 months of continuous gas consumption.

The example of unauthorized tampering into the pipe line.

Fig.4. Unauthorized tampering into the gas distribution pipeline.

Figure 4 illustrates the example of siphoning off gas. This example highlights the significant increase of gas explosion, because this pipe connection will not have periodic tests.

29/12:10	-2.48	3.89554	1.09108	608.0	2493.5	0.0
30/12:10	0.66	3.58011	1.09108	442.0	1843.0	0.0
31/12:10	-0.01	4.01907	1.09108	417.0	1740.3	0.0
01/01:10	1.11	4.04541	1.09108	377.0	1571.0	0.0
02/01:10	0.03	4.07455	1.09108	521.0	2215.1	0.0
03/01:10	-0.02	4.06241	1.09108	410.0	1723.2	0.0
04/01:10	-1.04	3.97841	1.09108	92.0	386.2	0.0
05/01:10	2.42	4.09960	1.09108	0.0	0.0	0.0
06/01:10	1.39	4.08296	1.09108	0.0	0.0	0.0
07/01:10	0.66	4.07565	1.09108	0.0	0.0	0.0
08/01:10	-0.14	4.05199	1.09108	0.0	0.0	0.0
09/01:10	-0.68	3.62364	1.09108	0.0	0.0	0.0
10/01:10	-0.40	2.89838	1.09108	0.0	0.0	0.0
11/01:10	-2.51	3.67092	1.09108	840.0	3259.4	0.0
12/01:10	2.24	3.67092	1.09108	819.0	3119.9	0.0
13/01:10	2.06	3.67092	1.09108	792.0	3024.2	0.0
14/01:10	1.72	3.67092	1.09108	917.0	3499.4	0.0
15/01:10	1.40	3.67092	1.09108	915.0	3498.1	0.0
16/01:10	6.57	3.67092	1.09108	818.0	3069.0	0.0
17/01:10	3.41	3.67092	1.09108	824.0	3138.5	0.0
18/01:10	-1.35	3.67092	1.09108	1390.0	5369.6	0.0
19/01:10	-0.27	3.67092	1.09108	1022.0	3939.3	0.0
20/01:10	1.99	3.67092	1.09108	871.0	3322.6	0.0
21/01:10	1.01	3.67092	1.09108	909.0	3481.9	0.0
22/01:10	1.91	3.67092	1.09108	877.0	3344.2	1.0
23/01:10	2.88	3.67092	1.09108	911.0	3463.6	0.0
24/01:10	0.75	3.67092	1.09108	923.0	3534.8	0.0
25/01:10	1.94	3.67092	1.09108	831.0	3173.5	0.0
26/01:10	3.27	3.67092	1.09108	811.0	3087.5	2.0
27/01:10	1.11	3.67092	1.09108	948.0	3625.8	0.0
28/01:10	2.57	3.67092	1.09108	810.0	3092.3	3.0
29/01:10	4.92	3.67092	1.09108	654.0	2470.8	0.0
30/01:10	3.72	3.67092	1.09108	686.0	2611.5	0.0
31/01:10	2.56	3.67092	1.09108	875.0	3328.7	0.0
01/02:10	2.14	3.67092	1.09108	841.0	3204.5	0.0
02/02:10	3.37	3.67092	1.09108	751.0	2851.3	0.0
03/02:10	4.42	3.67092	1.09108	911.0	3441.3	0.0
04/02:10	4.37	3.67092	1.09108	775.0	2925.3	0.0
05/02:10	2.51	3.67092	1.09108	734.0	2801.4	0.0
06/02:10	1.25	3.67092	1.09108	1333.0	5102.8	0.0
07/02:10	3.70	3.67092	1.09108	1084.0	4120.6	0.0
08/02:10	5.74	3.67092	1.09108	1263.0	4763.9	0.0
09/02:10	2.34	3.67092	1.09108	1375.0	5235.4	0.0
10/02:10	1.44	3.67092	1.09108	1319.0	5039.1	0.0
11/02:10	2.84	3.67092	1.09108	1259.0	4784.9	0.0

Fig.5. Interference in gas metering.

Figure 5 shows the interference in gas counter data, the aim of which is the decrease of gas metering, which leads to the lack of funds for environmental remediation.

5. Discussion and Conclusion

As a result of this research, we have developed the siphoning off gas Markov model. One of the findings to emerge from this study is that the modern intruder has learnt to set the additional unauthorized branch connections and to decrease the gas metering using virus. A tampering into gas distribution net highly increases the possibility of environmental damage such as gas explosion, corrosion and fires. Using virus to reduce gas metering leads to the lack of funds for environmental remediation. Consequently, the building of gas distribution net threat attack system is of highest interest. It is important to highlight that mathematical threat attack models can be based on database and information systems protection analysis models.

Reference

1. URL: https://ggf.bsu.edu.ru/Conferences/Conf_2011/Materials/Gribanov.htm (Date 12/10/2020)
2. Ejofodomi, O., & Ofualagba, G. *Automated volume measurement, adulteration detection, and tracking ofpetroleum products.* Paper presented at the Society of Petroleum Engineers - SPE Nigeria Annual International Conference and Exhibition 2020, NAIC 2020.
3. Ofualagba, G., & Ejofodomi, O. *Automated oil and gas pipeline vandalism detection system.* Paper presented at the Society of Petroleum Engineers - SPE Nigeria Annual International Conference and Exhibition 2020, NAIC 2020.
4. Visalakshi, P., Rohith, M., & Surya, C. *Fuel theft protection and management system.* International Journal of Advanced Science and Technology, 29(6),2020, pp.2606-2612.
5. Yang, X., Yi, X., Chen, S., Ruan, S., Zhang, J., Zheng, Y., & Li, T. *You are how you use: Catching gas theft suspects among diverse restaurant users.* Paper presented at the International Conference on Information and Knowledge Management, Proceedings, 2020. pp.2885-2892. doi:10.1145/3340531.3412751
6. Akimoto, T., Barkai, E., & Radons, G. *Infinite invariant density in a semi-markov process with continuous state variables*. Physical Review E, 101(5), 2020. doi:10.1103/PhysRevE.101.052112
7. Kouřim, T., & Volf, P. *Discrete random processes with memory: Models and applications.* Applications of Mathematics, 65(3), 2020.pp. 271-286. doi:10.21136/AM.2020.0335-19
8. Ortu, M., Conversano, C., Marchesi, M., Tonelli, R., Counsell, S., & Destefanis, G. *Describing software developers affectiveness through markov chain models.* Electronic Journal of Applied Statistical Analysis, 13(1), 2020. pp. 96-127. doi:10.1285/i20705948v13n1p96
9. Xu, Z., Ni, H., Reza Karimi, H., & Zhang, D. *A markovian jump system approach to consensus of heterogeneous multiagent systems with partially unknown and uncertain attack strategies.* International Journal of Robust and Nonlinear Control, 30(7),2020. pp. 3039-3053. doi:10.1002/rnc.4923
10. Yang, W., Deng, M., Tang, J., & Jin, R. *On the use of markov chain models for drought class transition analysis while considering spatial effects*. Natural Hazards, 103(3),2020. pp. 2945-2959. doi:10.1007/s11069-020-04113-6