Environment. Technology. Resources, Rezekne, Latvia
Proceedings of the 11th International Scientific and Practical Conference. Volume III, 310-315

Spurious Activation Assessment of Thermal Power Plant's Safety-Instrumented Systems

Sergei Trashchenkov[1], Victor Astapov[2]
Pskov State University, Computer Science and Electric Power Engineering Faculty, Tallinn University of Technology, School of Engineering[1],
Tallinn University of Technology, School of Engineering[2]

***Abstract.** Safety-instrumented systems (also called technological protections) play the significant role in prevention and mitigating of major accidents that can occur on thermal power plant. Activations of safety-instrumented system turn the power unit into safe state by shutting it down or reducing it productivity. The power generation process operates continuously. Any unplanned outage of generation equipment leads to undersupply of energy and big commercial losses to generation company. In Russia the values of allowed spurious trip rate for safety-instrumented systems are set by regulatory agency. These values are strict to all technological protections and do not take into account the differences in amounts of losses. This paper presents more flexible approach based on the Farmer's risk criterion. Also risk reduction factor for spurious activation is proposed.*

***Keywords:** Farmer's risk criterion, safety-instrumented systems, spurious activation, thermal power plant.*

I. INTRODUCTION

Nowadays thermal power plants (TPPs) are well studied facilities. Decades of operation in thousands of units all around the world produced data for technology development and great amount of studies. Part of those studies are dedicated to reliability issues.

Redundancy of important equipment for safety and reliability is the topic of [1]. The decision about necessity of installing additional lubricate oil pump in these study is based on decision tree approach and costs assessment.

Many papers are focused on maintenance activities. For example, [2] presents genetic algorithm with simulated annealing optimization method. Method helps in increasing reliability and reduce maintenance costs due to changing intervals of planned outages in depending on load demand.

Several papers are about safety-instrumented systems (SIS). In [3] the industrial experience of using IEC 61508 [4] in the thermal power plants is discussed. It was concluded that in most cases TPP equipment does not require very high level of reliability of SIS. In [5] concepts of IEC 61508 was used for Furnace Safety Supervisory System (FSSS) of TPP. Reliability of FSSS was improved by implementing redundant actuator.

Standard [4] uses SIS indexes of unavailability to response on demand (average probability of failure on demand or average frequency of failure) as a measure of reliability to promote the safety state of facility. Failure on demand can lead to the accident. Spurious failures in this approach are not taken into account because the result of such failures is safety state (shutdown or reduced productivity). In case of power plant such unplanned unavailability or reduced availability lead to big commercial losses. That is why assessment of spurious failures is crucial to TPP. The authors did not find any studies about TPP SIS spurious failures. Research of SIS spurious failures reliability in general is presented in paper [6]. Different approaches of computing spurious trip rate (STR) are described. In addition, the concept of spurious trip levels (STL) is criticized for economical point of view without any assessing of influence to the safety.

This paper introduces the approach for determine acceptable values of STR based of the potential amounts of losses.

II. MATERIALS AND METHODS

A. SIS description

SISs play significant role in accident prevention and mitigation of its consequences for hazardous facilities such as TPP. They perform safety functions by controlling the critical parameters. Crossing the thresholds by those parameters create demands for the SISs to turn off the process of facility or for reducing the productivity.

The structure of SIS can be envisioned as it is shown on Fig. 1. SIS consists of sensors subsystem (S), logic solvers subsystem (LS) and final elements subsystem (FE). Subsystems form series structure. That means that failure of even one subsystem leads to failure of all system. SIS functioning in response to demands mode. Demands are produced by equipment under control (EUC) with frequency λ_{de}. In the case of TPP EUC are power unit itself, steam boiler, steam

ISSN 1691-5402

http://dx.doi.org/10.17770/etr2017vol3.2529

turbine, feedwater pumps, etc. [7]. The results of SIS activation can be shutdown, reduction to 50 % productivity, reduction to 30 % or shifting to the idle conditions. If demand occurs, SIS should react. Presence of demand and absence of reaction due to SIS failure lead to the accident. SIS's unavailability can be represented by probability of failure on demand (PFD) for SISs with rare demands (less than one demand per year) or by frequency of failure (PFH) if demands occur more often than once per year. The limits of acceptable/unacceptable level of failures on demand depend on results of risk analysis. Standard [4] recommends several qualitative, quantitative and semi-quantitative methods for risk analysis. Describing these methods is beyond of this paper.

Triggering of SIS without demand is a spurious failure. Probabilistic representation of spurious failures is spurious trip rate (STR).

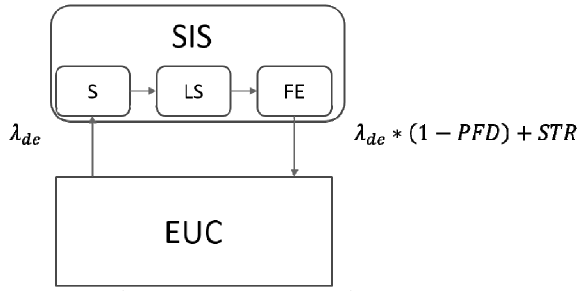

Fig. 1. Safety-instrumented system functioning (based on the concepts described in [4]).

Each subsystem can be designed with different redundancy. Redundancy usually represents as KooN (K out of N), where K is a number of subsystem's elements that is enough to trip subsystem; N is a total number of elements in the subsystem. In addition, K≤N. Subsystems with the same N and different K can have rather different reliability. Lower value of K makes subsystem more reliable to failures on demand just as higher value increases reliability to the spurious failures. Table 1 shows formulas for determining subsystem STR (according to the standard [8]). As it is clear from these formulas, STR values depend on several factors:

- reliability of elements (λ_S – spurious failure rate);
- mean time to repair/ restore (MTTR);
- percent of common cause failures (β_S).

o *STR risk acceptance criteria*

In the fundamental paper [10] risk R is described as triplet of scenarios s_i, probabilities p_i (or like in our case frequency f_i) and consequences x_i:

$$R = \{\langle s_i, f_i, x_i \rangle\}, \qquad (1)$$

where i=1, 2,…, N is a number of scenario.

Table I
Formulas for str of sis's subsystems with different redundancy [8]

Architecture	**Formula**
1oo1	$STR_{1oo1} = \lambda_S$
1oo2	$STR_{1oo2} = 2\lambda_S + \beta_s \lambda_S$
2oo2	$STR_{2oo2} = 2\lambda_S^2 + \beta_s \lambda_S$
2oo3	$STR_{2oo3} = 6\lambda_S^2 * MTTR + \beta_s \lambda_S$
2oo4	$STR_{2oo4} = 12\lambda_S^3 * MTTR + \beta_s \lambda_S$

Russian standard [9] requires strict values of STR for each SIS and the total value limitation for all SISs together (0.2 failure per year, no more than 0.065 failure per year for each SIS). The disadvantage of these reliability requiments is that it does not evaluate consequences of spurious trips.

Spurious shutdown or spurious reduced productivity leads to uncertain losses, which value depends on load demand. Authors introduce an risk-orientated approach to determine required values of STR based on load demand.

In our study, according to [9] and other standards, we assumed power unit with 38 SISs that spurious triggering leads to significant changes of availability. The SISs were grouped to consequences categories, as it is shown in Table II. For the sake of space full list is not presented in this paper.

Table II
Categories of SIS

Category of SIS	Amount of SIS
SISs that shut down the unit	28
SISs that reduce efficiency to 50 %	8
SISs that reduce efficiency to 30 %	1
SISs that turn unit into idle mode	1

Such form of risk can be represented in tabular form or graphically as a set of points on x-f-plane, There are two kinds of values to assess consequences x of spurious trip: amount of energy (MW*h) that is not produced due to spurious protection triggering (see Fig. 2). and amount of money losses (EUR). Amount of money losses is more preferable becouse of its ability to take into account several significant factors, such as changing of cost rate, operational and maintenance costs, penalties to system operator (the main expenditure). Graphical representation involves acceptance criteria (AC) [11]. AC can be straight line, curve or staircase function. The unit of STR is failures per year.

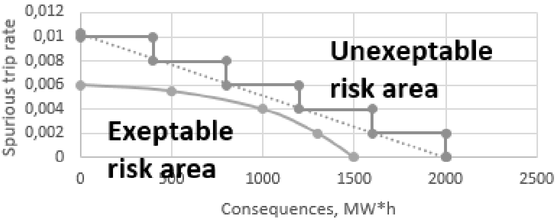

Fig. 2. Examples of the STR risk acceptance criteria.

In the case of straight line (on a logarithmic scale), risk criteria is equation [11]:

$$R_C = F \cdot X^m, \qquad (2)$$

where F are all values of frequency on risk criteria line; X are all values of consequences; m is a factor of proportionality.

Then we can implement risk reduction factor (RRF) to measure required improvements for SIS:

$$RRF_i = \frac{STR_U}{STR_A}, \qquad (3)$$

where STR_U is unacceptable STR of the SIS; STR_A is acceptable STR of the SIS.

SIS needs reliability improvements if it not satisfied to the risk criteria. For understanding the role of subsystems or even the role single elements in the total SIS reliability authors used importance measures [12].

B. Power unit description

One of the most important parameters of power plants operating on fossil fuel is input cost characteristic. Every generation unit (GU) is unique and has its own parameters, including fuel consumption, which depends on generation power. Generally, input cost characteristic *B(P)* can be represented as table or described by formula (4):

$$B(P) = a + bP + cP^2, \qquad (4)$$

where *a*, *b*, *c* – are coefficients of input cost characteristics; *P* – output power of GU; P_{min} – minimal amount of power that can be produced by GU. Fuel cost characteristic can show not only how much fuel consumes GU during one hour, but also show how much producer pays for one hour operation and measured in MW/MWh or €/h correspondingly.

The cost rate characteristic δ (P) evaluates how much fuel is necessary for production of 1 MWh or how much does it cost:

$$\delta(P) = B(P)/P\,. \qquad (5)$$

The efficiency characteristic *η (P)* of GU – is inversely proportional to cost rate characteristic value, and could be described in few words: the higher load – the higher efficiency.

$$\eta(P) = P/B(P)\quad. \qquad (6)$$

Fig 3 shows the example GU efficiency characteristic at TPP [13].

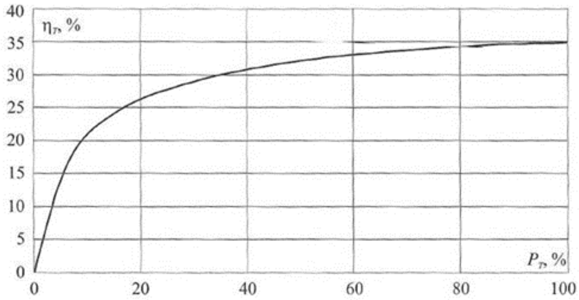

Fig. 3. The relation of GU efficiency from the load.

As result, every power plant, consisting on several GUs, has own optimal load dispatch according to the load profile and GUs' characteristics. In case of one GU, producer try to load it as much, as it possible. That is why some disturbances and changes in unit output lead to losses. Such kind of scenario could occur because of protection spurious triggering and as a result, GU need to reduce its output, unplug from the load or shut down.

With aim to evaluate consequences of the spurious triggering on power plant consisting of one GU, the authors considered following case. Fuel cost characteristics of GU are taken from [14] and presented in Table III.

Table III
Generators Data

Parameter				
$P_{min,}$ MW	$P_{max,}$ MW	a	b	c
30	200	208.4125	9.6506	0.0058

III. RESULTS AND DISCUSSION

A. Losses calculation

Let us assume that in normal regime the load of GU is 90% from nominal. In this case P_{G0} = 180 MW, and according to (4-5) the cost rate characteristic is δ_0 = 11.85 €/MWh.

Due to the fault, the output of GU changes to 0.5 P_{nom} = 100 MW. As result fuel consumption is changing and fuel price for production δ_1 = 12.31 €/MWh. Depending on restoration time, producer fuel consumption losses appear only because of less effectiveness. It means, that producer lost 0.46 € for every generated 1 MWh with total losses of 83 € per restoration hour.

We can see that fuel cost losses are not significant. However, we need to remember, that in this case, producer pays for other operational and maintenance costs such salary and own needs as well as do not sell electricity. For example, according to [15] the fixed operational and maintenance costs are 913 €/h. Total amount of generation losses is 996 €/h.

The most significant problem is, that according to nowadays conditions in electricity market, a producer have official duties to provide electricity to customers or system operator. In case of supplier default, it is obliged to compensate for the expenses incurred. Usually, this amount is registered in the contract. In our case, we consider general numbers taken from [16], where producer pays 0.77 € per none-provided kWh in case of interruption less than 48 hours. In case of generation reduction to $0.5P_{nom}$, the total unsupplied energy is ΔW = 80 MWh, it means, that compensation might be paid is 61 600 €.

Based on these two statements, the Table IV shows possible losses during protection spurious triggering different for scenarios.

The same way calculations for scenarios 2 and 3 are performed and presented in Table IV. Here generation costs are equal, because we assume, that fuel consumption in minimal margin is the same as without load, because generator should rotating.

Table IV
Possible Losses During Fault

№	Regime's changes	Repair duration, h	Generation costs losses, €	Fine to system operator, €	Total, €
1	90 % -> 0.5 P_{nom}	1	996	61600	62596
2	90 % -> P_{min}	1	1 206	100100	101306
3	90 % -> 0 %	1	1 206	138600	139806
4	90 % -> shut down	2	1826	277200	279026

As mentioned before, the time of restoration is varying, but in these particular calculations is taken as one hour for pp. 1-3. Most of the technologies have a limitations regarding to the minimum "rest" time before restarting. If the GU shuts down, the time of restoration is taken as two hours according to the average data for hot start presented at [15]. Here authors apply hot start, because of technology stopped less than 8 hours.

The results show, that TPPs consisting of one GU is very dependent from faults and protection spurious triggering due to high penalties for none supply. Obviously, it is especially critical for TPPs with bigger capacities. That is why there is a reason in additional agreements with more solid producers, who can provide reserve for less money. Installation of second GU, which increase costs (especially investment expenditures), but reduce possible penalties is an alternative option.

B. *Construction of risk acceptance curve*

According to [17], risk curve construction procedure includes following steps:

- collect relevant data and sort it by the value of consequences;
- calculate the cumulative function;
- show results as diagram.

As we mentioned above, existing reliability requirements [9] establish strict value for the summary STR that is equal to 0.2 failure per year without analysis of consequences. Authors assumed this value as a cumulative STR for the risk acceptance criteria.

Cumulative STR was divided equally to each of four SIS categories from Table II. Individual acceptable STR for single SIS depends on the number of SIS in each category. The values of potential losses, values of STR for single SIS of each category and cumulative STR are presented in Table V.

Table V
Categories of SIS with ranged consequances and cumulative STR

SIS category	Consequences	STR for the single SIS	Cumulative STR
SISs that reduce efficiency to 50 %	62596	0.001786	0.001786
SISs that reduce efficiency to 30 %	101306	0.00625	0.008036
SISs that turn unit into idle mode	139806	0.05	0.058036
SISs that shut down the unit	279026	0.05	0.108036

Diagram in Fig. 3 shows cumulative STR of data in Table V.

Assume the SIS that triggering lead to shut down of GU. As an example, we chose a SIS of controlling pressure in lubricate oil system of turbine. Reliability parameters of SIS's elements for spurious triggering and architectures of subsystems are in Table VI. Total value is computed by using formulas in Table I.

Table VI
Reliability parameters of SIS's elements

Element	**λ_S, 1/hour**	**Architecture**	**STR, 1/year**
Controller	0.0000057	1oo2	0.005
Pressure transmitters	0.0000002	2oo3	0.000183
Solenoid actuated valve	0.00000423	1oo2	0.00371
Total			0.008893

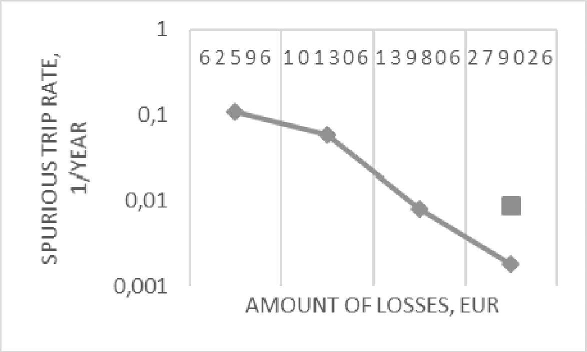

Fig. 3. Cumulative consequences-frequency curve of STR.

Obtained value of the SIS's STR is also presented in Fig. 3 as a single point. Result is unacceptable according to constructed risk acceptance curve. To make it acceptable based on (3):

$$RRF = \frac{0.008893}{0.001786} = 4.98\,. \qquad (7)$$

That means that obtained STR goes beyond the acceptable value in five times and should be reduced significantly by changing the elements or the architectures of subsystems.

Another way to construct risk acceptance curve is to use power function formula (8) and two scenarios, which STR and amount of losses assumed as acceptable [17].

$$F(L) = aL^{-b}\,, \qquad (8)$$

where a, b > 0 are parameters of the curve, L is amount of losses.

Consider two points of the future risk acceptance curve:

$$\begin{aligned} F(65000) &= 0.1, \\ F(120000) &= 0.01. \end{aligned} \qquad (9)$$

These points are rather close to points on acceptance criteria curve in Fig. 3. Parameters a and b can be found as:

$$\begin{aligned} 10^{-1} &= a \cdot 65000^{-b}, \\ 10^{-2} &= a \cdot 120000^{-b}. \end{aligned} \qquad (10)$$

Both equations include parameter a. After rearrangement the equation with unknown parameter b is:

$$\begin{aligned} 2^{b} &= 10, \\ b &= \log_2 10 = 3.322. \end{aligned} \qquad (11)$$

With known value of parameter b, parameter a is equal to:

$$a = \frac{10^{-1}}{60000^{-3.322}} \approx 746480476726256\,. \quad (12)$$

Risk acceptance curve can be described by the formula (13):

$$F(L) = 746480476726256 \cdot L^{-3.322}\,. \quad (13)$$

Graphical representation of equation (13) in linier scale is presented in Fig. 4. Any value of losses can by examined for maximum acceptable STR value by function (13).

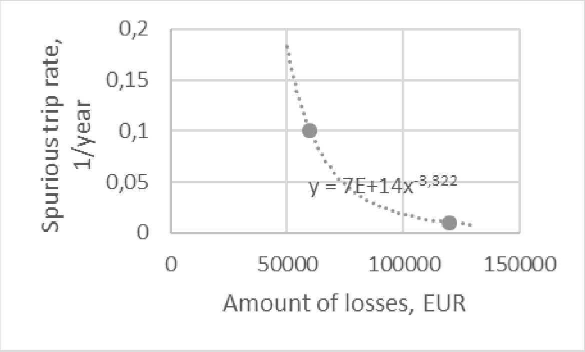

Fig. 4. Example of acceptable STR curve.

IV. CONCLUSION

In this paper, we introduced technique of spurious trip assessment for SIS of thermal power plants. We showed that our technique is more flexible than traditional one [9] and is compatible with it. It can be used as an addition to PFD assessment to improve the decision making process by taking into account such factors as effectiveness of GU regime, fuel costs, maintenance cost and penalties to the system operator.

V. ACKNOWLEDGMENTS

This publication is partially supported by European Regional Development Fund Higher Education Internationalisation, Mobility and Sustainability support program Dora Plus 2014-2020.4.01.16-0025 (contract 36.9-2/59).

REFERENCES

[1] Carazas, F. G., and Gilberto Francisco Martha de Souza. "Risk-based decision making method for maintenance policy selection of thermal power plant equipment," Energy, vol. 35.2, pp. 964-975, 2010.

[2] Leou, Rong-Ceng. "A new method for unit maintenance scheduling considering reliability and operation expense," International Journal of Electrical Power & Energy Systems, vol. 28.7, pp. 471-481, 2006.

[3] P. Rieff, R. Scholing "Power plants in a new safety perspective | Power Engineer," February 21 2013. [Online]. Available: http://www.engineerlive.com/content/24229 [Accessed: February 21, 2017].

[4] IEC 61508 Functional Safety of Electrical/electronic/programmable Electronic Safety-related Systems. International Electrotechnical Commission, - Geneva, 2010.

[5] Wang, Peng, Xiaoyan Chen, and Lei Yu. Application of Functional Safety Theories in Furnace Safety Supervisory System. 2017 9th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), January 14-15, 2017, Changsha, Hunan, China, pp. 164-167, 2017.

[6] Jigar, Abraham Almaw, Yiliu Liu, and Mary Ann Lundteigen. "Spurious activation analysis of safety-instrumented systems," Reliability Engineering & System Safety, vol. 156 pp. 15-23, 2016.

[7] Trashchenkov, S., & Egorov, V. *Analysis of emergency situations on the process of thermal power plants using mathematical apparatus of Petri nets. In Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference*, June 2015, Rezekne, Latvia, vol. 2, pp. 307-311, 2015.

[8] ISA TR 84.00.02. Safety instrumented functions (SIF) safety integrity level (SIL) evaluation techniques. Part 2: determining the SIL of A SIF via simplified equations. Technical report. Instrumentation, Systems, and Automation Society, Research Triangle Park, NC; 2002.

[9] RD 34.35.124 Technical Requirements for Reliability of Process Protective Means for 800 MW Power Units. ORGRES, - Moscow, 1993.

[10] Kaplan, Stanley, and B. John Garrick. "On the quantitative definition of risk," Risk analysis, vol. 1.1, pp. 11-27, 1981.

[11] Wang, J. C. et al. *Risk Criterion and Index of Risk. International Topical Meeting on Probabilistic Safety Assessment (PSA'96)*, September 29-October 3, 1996, Park City, UT, 1996.

[12] Van der Borst, M., and H. Schoonakker. "An overview of PSA importance measures," Reliability Engineering & System Safety, vol. 72.3 pp. 241-245, 2001.

[13] M. Valdma, H. Tammoja, and M. Keel, *Optimization of Thermal Power Plants Operation*. Tallinn: TUT press, 2009.

[14] M. Valdma, M. Keel, H. Tammoja, and J. Shuvalova, “Economical Dispatch of Power Unit under Fuzziness,” vol. 24, no. 2, pp. 249–263, 2007.

[15] K. Engblom, “Features and parameters of various power plant technologies,” *Detail. Wärtsilä’s Tech. Mag.*, no. 2, pp. 1–67, 2014.

[16] “Network service quality requirements and network fees conditions in case of violation,” *Võrguteenuste kvaliteedinõuded ja võrgutasude vähendamise tingimused kvaliteedinõuete rikkumise korral*, 2016. [Online]. Available: https://www.riigiteataja.ee/akt/1039867?leiaKehtiv. [Accessed: 12-Feb-2017].

[17] Häring, Ivo, *Risk Analysis and Management: Engineering Resilience*. Springer, 2015.