Zhulina Svetlana, Kuznetsova Tatiana
Rostechnadzor, Moscow, Russia

Kostogryzov Andrey
Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences, Moscow, Russia

Kurpatov Oleg
The Russian Corporation of Communication Devises, Moscow, Russia,

Nistratov Andrey, Nistratov George
Research Institute of Applied Mathematics and Certification, Moscow, Russia

The probabilistic analysis of the remote monitoring systems of critical infrastructure safety

Keywords

information, model, monitoring, probability, risk, safety, system, technology

Abstract

The approach for probabilistic analysis of the remote monitoring systems (RMS) of critical infrastructure safety (CIS) is proposed. It allows to estimate the reliability and timeliness of information producing, the completeness, validity and confidentiality of the RMS information. In application to composed and integrated CIS with RMS and without RMS the earlier models, developed by authors, are used. The methods for evaluating influence of RMS quality on risk to lose CIS integrity are developed. Some effects of RMS applications in Russia are demonstrated.

1. Introduction

The usual approaches to critical infrastructure safety (CIS) which have developed in last dozen years (in the oil and gas and chemical industry, in coal branch, etc.), based in many respects on subjective safety estimations «on places», have reached a high but not sufficient level of efficiency. For the account of interests of all interested parties and the further business development today a rethinking system possibilities of applied information technologies for increasing safety and extracting the innovative effects which are not used fully till now.

Search of cardinal directions of improving CIS, favourable to business and the state, has led to comprehension of sharp necessity and expediency of creation and implementation of remote monitoring system (RMS). RMS transforms an internal information support of separate CIS in a mode of a needed transparency and wide availability of CIS state in real time for all interested and responsible parties. Along with it on the basis of rational RMS implementation the transition from the existing subjective expert approach to the risk-based approach for critical infrastructure safety receives necessary information filling.

The proposed probabilistic analysis of RMS operation in their influence on integral risks to lose system integrity is based on researching real remote monitoring systems implemented in Russia for oil and gas CIS. In application to composed and integrated CIS with RMS and without RMS the earlier models, developed by authors, are used [1-10]. The received results are applicable for an analytical rationale of system requirements to RMS, system definition of the balanced preventive measures of systems, subsystems and elements integrity support at limitations on resources and admissible risks.

2. About the general purpose of RMS operation and its evaluation

RMS is intended for a possibility of prediction and the prevention of possible emergencies,

minimization of a role of human factor regarding control and supervising functions. It may be reached on the basis of gathering and analytical processing in real time the information on controllable parameters of objects monitored. For example, objects monitored for oil and gas CIS are the technological equipment and processes of extraction, transportation, refining, the personnel, systems and means of safety support.

The role of RMS is defined by their functions, to basic of which concern (*see Figure 1*) :

remote continuous monitoring of CIS condition in real time (gathering data about key parameters of technological processes; gathering and processing data of industrial inspection, the information of technical condition and equipment diagnostics, the information on presence of failures and incidents and results of system recovery etc.);

analytical data processing;

prediction of risks to lose CIS integrity;

display of CIS conditions and predictions with necessary level of details.

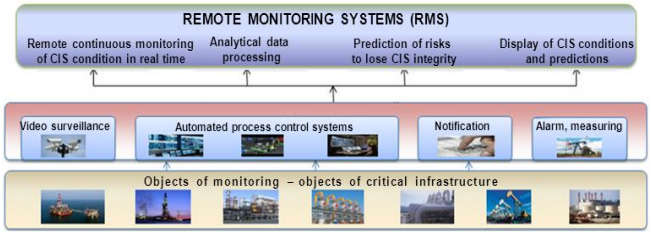

Figure 1. The purpose of RMS

Unlike the usual control which is carried out at enterprises (when the state supervising body in the field of industrial safety, and frequently also the enterprise/holding bodies of the industrial safety control receive the information only upon incident or failure, not possessing the actual information about deviations at an initial stage when still it is possible to prevent failure), RMS translates the control, a transparency of CIS conditions, the important real time information (about the facts and predictions), and also necessity of proper response to critical deviations for absolutely new time scale characterized as scale of real time, measured by seconds-minutes.

Thus, in general system application of RMS, subsystems and system elements always aims to provide reliable and timely producing the complete, valid and, if needed, confidential information for its proper further pragmatical use [2-4, 13]. And potential threats realization worsens the used information – see *Figure 2.*

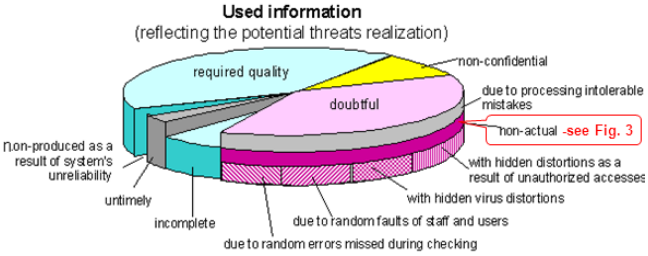

Figure 2. Potential threats to used information according to general purpose of RMS operation

On Figure 3the example of invalid information kept in RMS is rereflected. Because of inadequate data gathering or because of failure RMS source element or because of human mistake or the bad data checking etc. the wrong information about a "normal" condition of the equipment is reflected in RMS data base (by green arrows from sources) while the emergency is in a reality (red equipment, i.e. arrows from sources should be red instead of green). As concequence reaction on emergency is not activated in time. It means the system of information gathering in such RMS does not meet the purpose requirements!

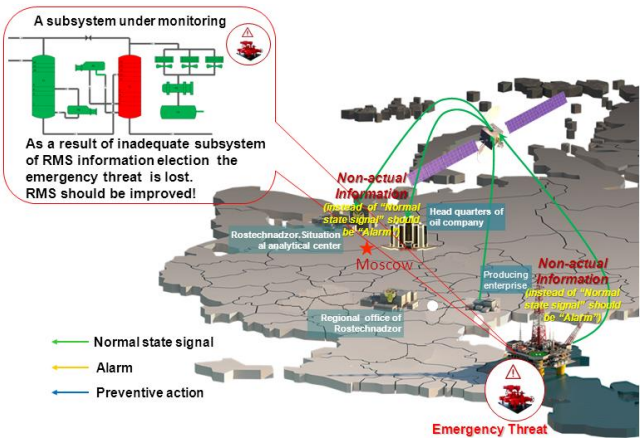

Figure 3. Example of invalid information kept in RMS because system of information gathering does not meet the purpose requirements

The example about gathering the actual information in RMS according to a real equipment state deviation is on *Figure 4* (condition in RMS database according to yellow arrows corresponds to a real condition, reflected also by yellow color of equipment). As concequence reaction on deviation is activated in real time (blue arrow).

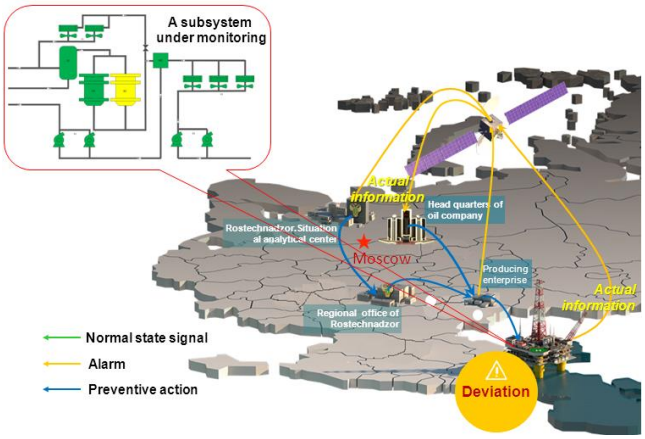

Figure 4. Example of invalid information kept in RMS because system of information gathering does not meet the purpose requirements

Effects from the remote control can be reached only when quality of RMS operation is provided. It means reliable and timely producing the complete, valid and, if needed, confidential information by RMS.

In general case a probabilistic space (Ω, B, P) for an evaluation of system operation processes is proposed, where: Ω - is a limited space of elementary events; B – a class of all subspace of Ω-space, satisfied to the properties of σ-algebra; P – a probability measure on a space of elementary events Ω. Because, $\Omega=\{\omega_k\}$ is limited, there is enough to establish a reflection $\omega_k \rightarrow p_k = P(\omega_k)$ like that $p_k \geq 0$ and $\sum_k p_k = 1$. Such space (Ω, B, P) is built [1-12] and proposed for RMS evaluation because RMS may be considered as specially focused information system (IS). The proposed analytical models and calculated measures are the next [1-10, 13]:

"The model of functions performance by a complex system in conditions of unreliability of its components" (the measures: T_{MTBF} - the mean time between failures; $P_{rel.}(T_{given})$- the probability of reliable operation of IS, composed by subsystems and system elements, during the given period T_{given}; $P_{man}(T_{given})$ - the probability of providing faultless man's actions during the given period T_{given});

"The models complex of calls processing (the measures for the different dispatcher technologies (for unpriority calls processing in a consecutive order for singletasking processing mode, in a time-sharing order for multitasking processing mode; for priority technologies of consecutive calls processing with relative and absolute priorities; for batch calls processing; for combination of technologies above): the mean wait time in a queue; the mean full processing time, including the wait time; P_{tim} - the probability of well-timed processing during the given time; the relative portion of all well-timed processed calls; the relative portion of well-timed processed calls of those types for which the customer requirements are met C_{tim});

"The model of entering into IS current data concerning new objects of application domain" (the measure: P_{compl} - the probability that IS contains complete current information about states of all objects and events);

"The model of information gathering" (the measure: $P_{actual.}$ - the probability of IS information actuality on the moment of its use);

"The model of information analysis" (the measures: P_{check} is the probability of errors absence after checking; the fraction of errors in information after checking; $P_{process}$ - the probability of correct analysis results obtaining; the fraction of unaccounted essential information);

"The models complex of dangerous influences on a protected system" (the measures: $P_{inf.l.}(T_{given})$ - the probability of required counteraction to dangerous influences from threats during the given period T_{given});

"The models complex of an authorized access to system resources" (the measures: P_{prot} - the probability of providing system protection from an unauthorized access by means of barriers; $P_{conf.}(T_{given})$ - the probability of providing information confidentiality by means of all barriers during the given period T_{given}).

These models, supported by different versions of software Complex for Evaluation of Information Systems Operation Quality, patented by Rospatent №2000610272 (CEISOQ+), may be applied and improved for solving such system problems in RMS life cycle as: substantiation of quantitative system requirements to hardware, software, users, staff, technologies; requirements analysis; estimation of project engineering decisions and possible danger; detection of bottle-necks; investigation of problems concerning potential threats to system operation and information security; testing, verification and validation of RMS operation quality; rational optimization of RMS technological parameters; substantiation of projects and directions for effective system utilization, improvement and development.

3. RMS as complex system. Evaluations

Generally system analysis of RMS operation consists in evaluation of reliability and timeliness, completeness, validity and confidentiality of the used information. In special cases for compound subsystems and system elements not all measures may be used. For example, for a subsystem of information security enough to use the measures to evaluate protection from an unauthorized access and

information confidentiality during the given time period. In dependence of the purposes of researching RMS can be decomposed to level of compound subsystems and separate elements – see *Figure 5.*

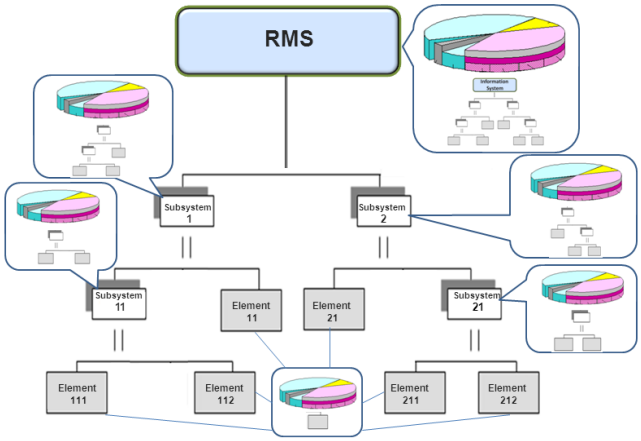

Figure 5. Decomposition RMS to level of compound subsystems and elements

In this case according system engineering principles the operation quality of every component should be evaluated.

For evaluating integral RMS operation quality the next measure is proposed: the probability of providing reliable and timely representation of the complete, valid and confidential information during the given time – $P_{RMS}(T_{given})$.

In general case
$P_{RMS}(T_{given}) = P_{rel.RMS}(T_{given}) \bullet C_{tim\ RMS} \bullet P_{compl..RMS} \bullet P_{actual..RMS} \bullet P_{check\ RMS} \bullet P_{process.RMS} \bullet P_{inf.l.\ RMS}(T_{given}) \bullet P_{man\ RMS}(T_{given}) \bullet P_{prot.RMS} \bullet P_{conf.RMS}(T_{given})$,
where all measures are calculated by the models, proposed in part 2.

For complex structures the ideas of combination of the models is proposed in [3-13]. It allows in an automatic mode to generate new models at the expense of what there is possible evaluation of the measures above.

4. Evaluation of influence of RMS quality on risk to lose CIS integrity

When not all system elements and subsystems are captured by RMS capabilities, two subsystems, operated in different time scale, are cooperated in the CIS. Part of CIS, captured RMS, is served in real time, and other part - in a usual time scale (with information gathering by a principle "as it is possible to receive"). In many critical situations this usual time scale cannot be characterized as adequate to a reality. With use of the offered approach the system with usual control (UC), used for CIS, i.e. without RMS application can be estimated. Generally the analyzed critical infrastructure is presented as a combination "System+RMS" and usual "System without RMS". And "System+RMS" is combination of "Structure for RMS" and "RMS" – see Figure 6. For these systems some measures of the information delivery may not answer requirements of real time - "System+RMS" because of RMS operation quality is inadequate and "System without RMS" because without RMS.

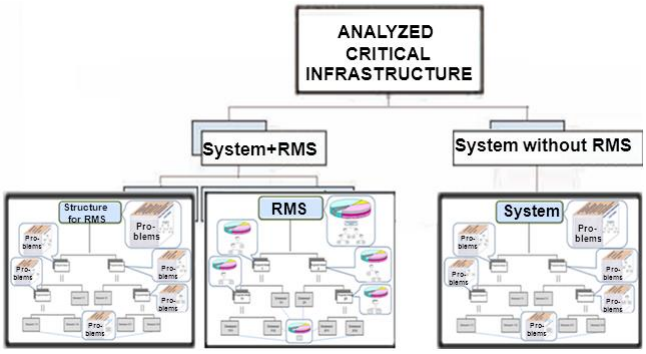

Figure 6. Decomposition of analyzed critical infrastructure to fill influence of RMS

All great number of the factors characterizing threats to analyzed critical infrastructure, is considered as 100 %, and total frequency of dangerous deviations is designated through $\lambda_{\sum}$. Frequency of potentially dangerous deviations traced by «System + RMS», is designated λ_{RMS}. Frequency of occurrence of other potentially dangerous deviations which are not traced by RMS (i.e. for «System without RMS»), it is designated $(\lambda_{\sum} - \lambda_{RMS})$.

For "System + RMS" the RMS operation quality during the time of prediction T_{given} is evaluated by probability $P_{RMS}(T_{given})$. And the risk of critical deviation for safety during the time of prediction T_{given}, designated as $R_{RMS}(T_{given})$, can be evaluated by the earlier methods [1-10, 13]. For the usual "System without RMS" the same measures $P_{UC}(T_{given})$, $R_{UC}(T_{given})$ can be used with specified value of input for probabilistic modelling.
Then in general form the risk $R(T_{given})$ to lose integrity for analyzed critical infrastructure during the time of prediction T_{given} can be evaluated by the formula:

$R(T) = 1 - [(\lambda_{RMS} / \lambda_{\sum}) P_{RMS}(T_{given}) (1 - R_{RMS}(T_{given})) + ((\lambda_{\sum} - \lambda_{RMS})/ \lambda_{\sum}) P_{UC}(T_{given}) (1 - R_{UC}(T_{given}))]$,
where expression in square brackets is a probability of successful operation of analyzed critical infrastructure. Depending on the made risk definition in special cases it can be interpreted as

probability of safe or reliable operation or probability of norms observance for critical parameters of the equipment or other in the conditions of associated potential threats. The case $\lambda_{\sum} = \lambda_{RMS}$ means full capture of critical infrastructure by RMS capabilities.

5. What about the pragmatic effects?

Authors of this article took part in creation of the Complex (as a part of global RMS) of supporting technogenic safety on the objects of oil&gas distribution and have been awarded for it by Award of the Government of the Russian Federation in the field of a science and technics for 2014. The created peripheral posts are equipped additionally by means of Complex to feel vibration, a fire, the flooding, unauthorized access, hurricane, and also intellectual means of the reaction, capable to recognize, identify and predict a development of extreme situations – see engineering decisions on *Figure 7.*

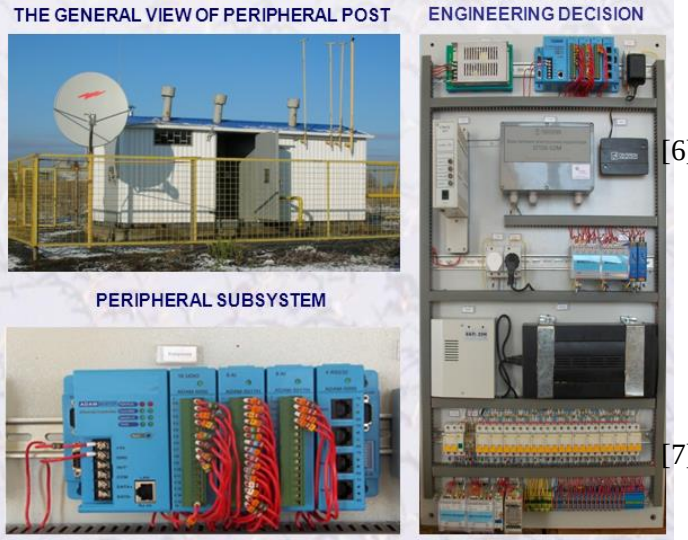

Figure 7. The Complex of supporting technogenic safety on the objects of oil & gas distribution

The applications of some Complex for 200 objects in several regions of Russia during the period 2009-2014 have already provided economy about 8,5 Billions of Roubles. The economy is reached at the expense of effective implementation of the functions of risks prediction and processes optimization [9].

References

[1] Kostogryzov, A.I., Petuhov, A.V. & Scherbina, A.M. (1994), Foundations for evaluation, providing and increasing output information quality in application to automatized systems. Moscow: "Armament. Policy. Conversion", 278p.

[2] Kostogryzov, A. (2000), *Software Tools Complex for Evaluation of Information Systems Operation Quality (CEISOQ).* Proceedings of the 34-th Annual Event of the Government Electronics and Information Association (GEIA), Engineering and Technical Management Symposium, 25-29 September, 2000, 63-70.

[3] Kostogryzov, A. & Nistratov, G. (2004). Standardization, mathematical modelling, rational management and certification in the field of system and software engineering", Moscow, Armament.Policy.Conversion, 395p. (in Russian)

[4] Kostogryzov, A.I. & Stepanov, P.V. (2008). Innovative management of quality and risks in systems life cycle, Moscow, Armament. Policy. Conversion, 404p. (in Russian)

[5] Kostogryzov, A., Nistratov, A. & Nistratov, G. (2012). Applicable Technologies to Forecast, Analyze and Optimize Reliability and Risks for Complex Systems. *Proceedings of the 6st International Summer Safety and Reliability Seminar*, Poland, Volume 3, Number 1, pp. 1-14, September 2012

[6] Kostogryzov, A., Nistratov, G. & Nistratov, A. (2012). Some Applicable Methods to Analyze and Optimize System Processes in Quality Management, *Total Quality Management and Six Sigma*, InTech, pp. 127-196. Available from: http://www.intechopen.com/books/total-quality-management-and-six-sigma/some-applicable-methods-to-analyze-and-optimize-system-processes-in-quality-management

[7] Kostogryzov, A., Grigoriev, L., Nistratov, G., Nistratov, A. & Krylov, V. Prediction and Optimization of System Quality and Risks on the Base of Modelling Processes", American *Journal of Operations Research*, Special Issue, Volume 3, Number 1A, pp.217-244, January 2013, Available from: http://www.scirp.org/journal/ajor/

[8] Kostogryzov, A., Nistratov, G. & Nistratov, A. (2013). The Innovative Probability Models and Software Technologies of Risks Prediction for Systems Operating in Various Fields. *International Journal of Engineering and Innovative Technology* (IJEIT), Volume 3, Issue 3, September 2013, pp. 146-155. *http://www.ijeit.com/archive.php*

[9] Kostogryzov, A.I. etc. (2015). Security of Russia. Legal, Social & Economic and Scientific & Engineering Aspects. The Scientific Foundations of Technogenic Safety Edited by N. Machutov – Moscow: «Znanie», 2015, - 936p.

[10] Kostogryzov, A.I., Stepanov, P.V, Nistratov, G.A., Nistratov, A.A., Grigoriev, L.I. & Atakishchev, O.I. (2015). Innovative Management Based on Risks Prediction. Information Engineering and Education Science – Zheng (Ed.). Taylor & Francis Group, London, ISBN 978-1-138-02655-1, pp. 159-166.

[11] Zio, E. (2006.) An Introduction to the Basics of *Reliability and Risk Analysis*, World Scientific, 2006, 222p.

[12] Kolowrocki, K. & Soszynska-Budny, J. (2011). *Reliability and Safety of Complex Technical Systems and Processes*, DOI:10.1007/978-0-85729-694-8, Springer-Verlag London Limited, 2011, 405p.

[13] Kostogryzov, A., Stepanov, P., Nistratov, A., Nistratov, G., Zubarev, I. & Grigoriev, L. (2016). Analytical modelling operation processes of composed and integrated information systems on the principles of system engineering. *Journal of Polish Safety and Reliability Association. Summer Safety and Reliability Seminars*, Volume 7, Number 1, 157-166. Available from: http://jpsra.am.gdynia.pl/archives/jpsra-2016-contents/