Knowledge Based Event-Oriented Approach in Control Systems

Vikentiev A.*, Vaguine A.*, Mikheev V**, Poluektov S.**
*- Moscow Radiotechnical Institute RAS, vaguine@inm.ras.ru
**- Altey Ltd, Moscow, altey@inm.ras.ru

1 Introduction

Safety control, alarm system and reliability of the big and complicated objects (accelerators, aviation, atomic power station and railway) is the field where the integrated knowledge base is importance both for strategic planning and for operative control. The analysis of the big data and information packages about the failures and the consequences for the complex system effective control takes a lot of time. In modern dialog complexes some part of the failure and incident data is taken from the real time data collecting system, the other part of this data is fixed in the inquiry files.

The real time data is usually needed for the on line control within the complex and practically not used as a source of the reliability and safety knowledge. On the other hand the inquiry file information about the incident cause and its consequences and about the following recommendations is very valuable but this non formal information is not ready for any statistical processing and generalization based on the thousand incidents. In the big systems only small part of such unformalised information is used for the reliability and safety control and is taken into account in the strategic planning of the control operations. The paper describes some approach to the formal description of the essential characteristics of the complex system comes from the incident inquiry and the event-oriented analysis technology to fulfill it. The information system related to existing monitoring systems to expand the control knowledge base using the formalized knowledge from inquiry files to plan prophylactic measures and to predict the situation is briefly discussed.

The basic system was used in practice since 1995.

2 Formal description of incidents

The main reason preventing on the formal incident description is the impossibility to point out the level of its detailization beforehand. From one side, the conditions of the incident might be rather clear but or completely muddled from the other side. It is absurd to describe all the details of the incident but it is also dangerous to lose any trifle.

So the structure of the formal incident description should be logically finished even for the initial description and should have unlimited possibilities to include many new details in it.

The analysis of some approaches to formal incident description (railway, aviation, power station, etc.) shows that the methods and forms now used restrict the list of incidents to be described as well as the level of detalization. That is why the experts did not use the formal description as a source of the knowledge to make decision and used it mostly for some statistics.

From our point of view the most suitable constructive form for the incident description in most applications is the cause-consequence network in which nods (event classes) are homogeneous and permitted to have a few possible sub-classes of each event (if there is no enough sub-classes to determine the event - used the class name).

In the case we used cause-consequence network structure with unified for all the incident scenario and realized as a joint type tree structure of the unfavorable events, classified to one of the classes:

- unstability factors of the system functioning;
- technical means failures;
- incorrect stuff actions;
- critical (dangerous) events;
- final events.

The initial sources of the incidents are inner or outer unstable factors of the functioning system. These factors lead to a technical means failures and cause an incorrect stuff actions, which successions and combination could cause some critical situation. The final failure may happen as a result of a the <<stored>> functional deviations within the system (Fig.1). Of course the final event should follow a diverge type event-consequences tree structure but the classifier of this part is not finished in development.

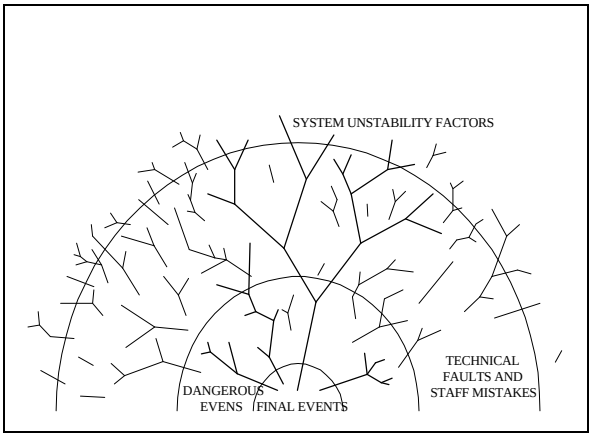

Fig. 1. Incident scenario.

The unit of the knowledge (and description) in relation-type data base about the subject is the quality information about the cause-consequence relations of one or a few cause-events with consequence-events. All the information about the cause-consequence relations taken from the incident descriptions is the homogeneous knowledge base about the ways of the incident start and progress.

The formal base of incident description in network structure is two type of classifiers:

- classifier of unfavorable events (net peaks);

- classifier of cause-consequence relations of event pairs (net arcs).

From the economical and methodical point it's very important both classifiers adopt the content of most of the existing in many fields classifiers of incidents, cause, factors, conditions and so on.

3 Unfavorable event classifier

One unit of the incident or breakage and the causes in most of the classifiers used in many industried branches is one unfavorable event which took place in one specific structure element of the system. Practically the classifier of the structure elements and the classifier of the types of unfavorable events could exist separately and in the case each unfavorable event will be a function of two dimension classifier (structure element – type of element). Such approach is used in the civil aviation for example. In the contrary the structure elements and types of events can be gathered in one linear type of classifier, which is supposed to consider all the combinations of the structure elements and types of events. This type of classifier was used in safety control of Russian railways and came into operation under the subjective conception of the incident formalization (the incident – the only one cause). Such approach was not possible to use for the development of cause-consequence networks but some formal points were used.

According to the incident progress scenario developed together with the field experts, our unfavorable event classifier consists of 5 classes of events regulated in the direction of the unfavorable event reconstruction from the consequences to the cause (the first figure of the number event) (Fig.2).

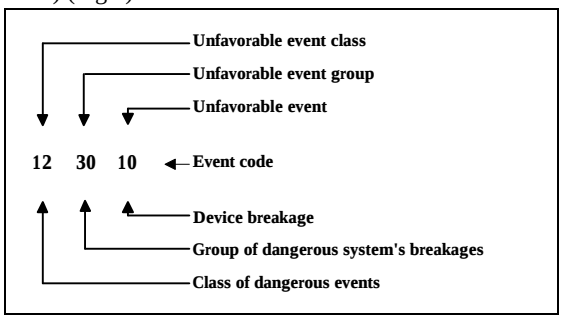

Fig. 2. Unfavorable event classifier.

Inside the classes the events referred to the kind of events which joint the events in the independent group (consequently the second and the third figures). Within the breakage class of technical devices the group collects all the breakage of certain technical devices, within the incorrect stuff actions the group collects all the incorrect actions of the certain function of the operators, within the class of dangerous events the group joints the dangerous events in connection with the certain source of the danger, in the class of the final events the groups are constructed by the events with the similar results, in the class of unstability factors the groups are formed according to the source of unstability.

At the moment our classifier consists of more then 1000 of unfavorable events and there are means to widen its capability both of the class numbers and of the hierarchy classes depth. For the time being we need up to 10^4 types of the events to describe the incidents.

4 Cause-consequence relation classifier

The cause-consequence relation classifier is developed as rectangular matrix with the lines and columns corresponding to the types of events taken from the unfavorable event classifier. The special sign in some element of the matrix means that there is cause-consequence relation between the type of event in the title of the line and the type of event in the title of the column(Fig 3).

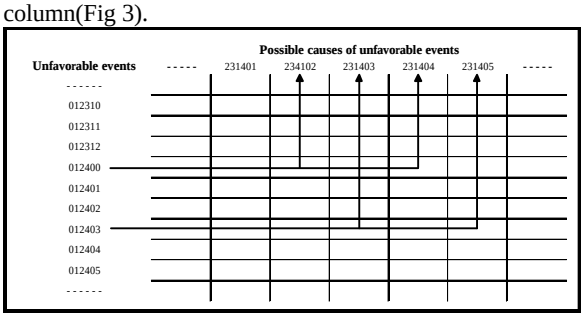

Fig. 3. Cause-consequence relation classifier.

The very event is not connected to itself, but there is no other restrictions to fulfill the matrix. The places of signs in the matrix are determined by the algorithm of the control system and are fixing the elementary knowledge of the control system about the incident initialization and progress. For the classifier size mentioned above we have about 10^6 element of matrix and need up to 10^8 for full system. For that reason we developed the special interface for experts to minimize the time and to simplify the procedure. But the main problem here is to develop an information technology to collect knowledge throng the using the complex and capacious filters (patterns).

5 Knowledge collection and use technology

The main idea of the knowledge collection and use technology is to use specialized interface to take the knowledge about the structural regularity of incidents each time when an inquiry team starts working. An inquiry team stuff working on the safety control of the big system is rather numerous and its working mode is very intensive.

We decided to add to the existing information network software comparably inexpensive software package to switch on all the experts to the infrastructure in real time to collect the data and knowledge of the incident investigation to the joint knowledge base and through the central knowledge base give them the knowledge for helping in everyday work (investigation, prophylactic measures planning, etc.). Experts working on the central knowledge base are following the knowledge base editing and systematizing the fragment of the knowledge base(Fig.4).

Our final target is to store in the knowledge base the

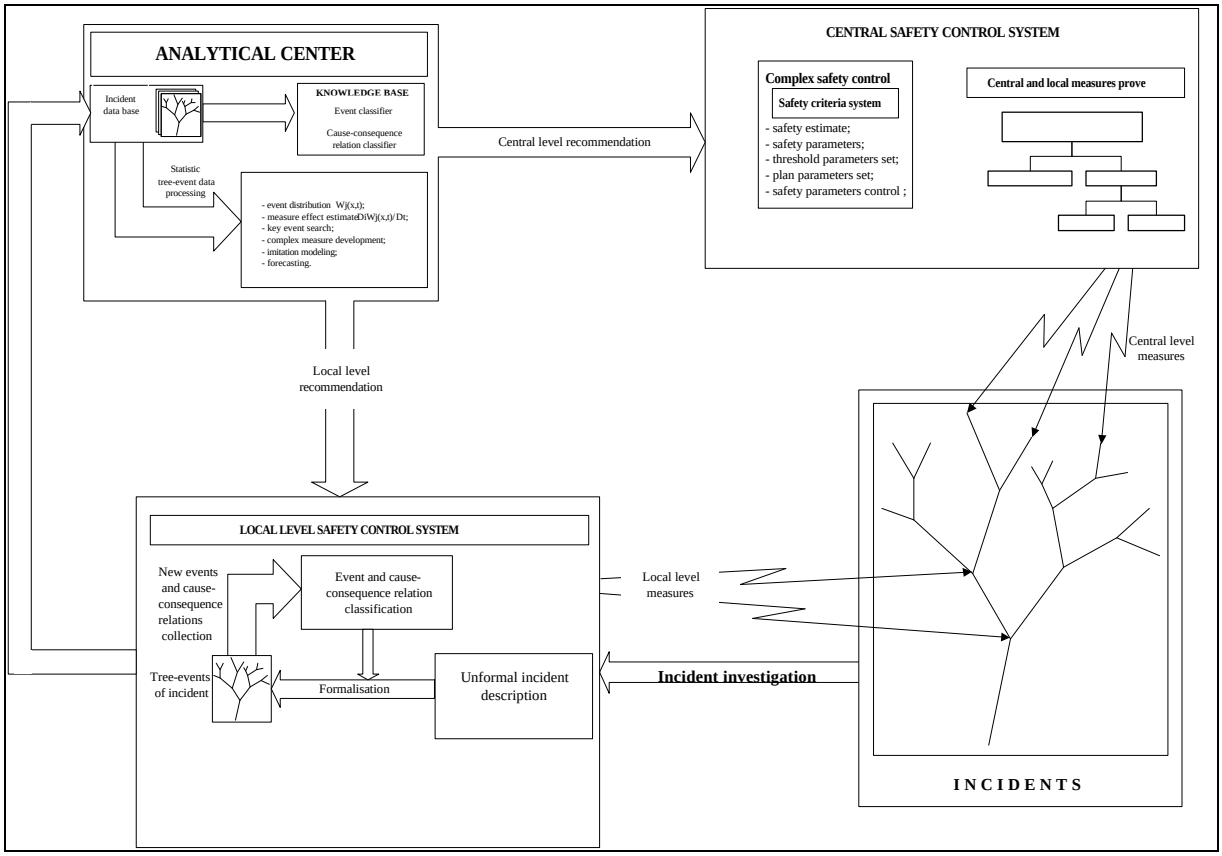

Fig. 4. Knowledge collection and use technology.

verity of events and cause-consequence relations to start describing the history of each event including the factors which are not in the list of factors taken into account by the safety control system. The details of the cause-consequence descriptions are determined as such a way to describe the prophylactic measure effect in future.

Our estimation of 10^4 formalized incidents per year and of 10 cause-consequence relation per incident gives us about 10^5 cause-consequence relations in the knowledge base per year.

6 Incident formal description

The software of the operator's interface for the incident formal description is included in the normal operator interface (data transfer, completing and transfer unformalized descriptions of incidents, operative data etc.) The operator is given rather very simple case technology to complete the unfavorable event tree structure. This interface is initializing the classifiers mentioned above offering him the suitable versions of event and relations. So the formal description of the incidents used earlier in the form of many attributes (place, time, type of incident etc.) and the cause unformalized description, obstacles, results of the incidents is added by the formal description of the incident as the cause-consequence network. The nods of the network are positioned in time and space of the unfavorable events, which took place either with the system objects or its media (technical means, stuff etc.).

The better developed the classifiers the more detailed and mattered the incident description becomes. The interface algorithm does not permitted the operator to go through a few levels of cause-consequence relations to check his inquiry.

The key point in the new knowledge collecting is the classifier adding mechanism. If during the investigation there will be some information absent in the classifiers the operator is capable to add the new types of events proved by the inquiry team. After this procedure the new types of events will be accessible to the other operators.

7 The central expert system

Using the formalized description of the events and measures is permitted to process the information in usual manner to use if for statistics, operative control and so on and it gives the "portability" of the information, but the new technology gives much more power in analysis and forecasting of the system functioning.

7.1 Statistical analysis of reliability and safety

The formal description of incident described gives us the possibility to analyze the statistics of the accompanied hidden causes and the key events. At the time being in the

system realized are:

- automatic seeking of the key events on the whole numaryty of the cause-consequence structures of the incidents;
- ranging of unfavorable events on the dangerous base and its percentage to the total number of incidents;
- determining the risk incident mean value of for any fixed structure on the base of the generalizing of the incident cause-consequence regularity of the.

7.2 Safety estimation

For the moment there are a tenth of technical or economical criteria′s of safety for the complex social-technical systems but no one of them is complete. In our system an adoptive approach was developed for the safety estimation. To support an open adaptive criteria it uses T.Saaty's method of the hierarchic analysis [2]. Within the method the dialog system was developed within which an expert creates and adopts the complex criteria as a function of the collected data and knowledge as well as in combination with some criteria already exist. As a result there is a new system of hierarchic criteria to control a state of safety on the base of the threshold and planned meaning of one or a few basic criteria.

7.3 Forecast and measures development

An imitation model is used to forecast the safety of the system. The object for imitation is the ties and transitions between the unfavorable events which leads to the incidents. The model uses the structural regularity from the knowledge base taking into account both the frequency of the unfavorable events and the probability of the cause-consequence transfers. For that reason the system calculates in regular manner:

- probability of the events;
- probability of the cause-consequence transfers;
- correlation of probability of different cause complex of the event;
- distribution of the types of unfavorable events in time and space;
- effect estimate of the measures as a function of the cause- consequence probability.

The main target of modeling is to estimate the influence inner or outer parameters of the safety state and an estimate of the prophylactic measures.

8 Conclusion

The approach described in the paper was put into operation for the Russian railway safety control system to analyze more then 10^4 incidents per year. The information technology in combination with the advanced mathematical analytical methods and the three level classifier gave to clear the dangerous situations and to pick up the parameters of the safety system.

References

[1] M. Beharrell, G. Benincasa, J.M. Bouché, J. Cuperus, M. Lelaizant, L. Merard, Model based, detailed fault analysis in the CERN PS complex equipment, ICALEPCS'95, FERMILAB, Proc. 1995, p.474.

[2] Thomas L. Saaty, Kevin P. Kearns Analytical Planning. The organization of Systems, Pergamon Press, New York, 1985.